



HAL
open science

Invariant Algebraic Sets and Symmetrization of Polynomial Systems

Evelyne Hubert

► **To cite this version:**

Evelyne Hubert. Invariant Algebraic Sets and Symmetrization of Polynomial Systems. Journal of Symbolic Computation, 2019, 95, pp.53-67. 10.1016/j.jsc.2018.09.002 . hal-01254954v4

HAL Id: hal-01254954

<https://inria.hal.science/hal-01254954v4>

Submitted on 25 Sep 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Invariant Algebraic Sets and Symmetrization of Polynomial Systems

Evelyne Hubert *

Abstract

Assuming the variety of a polynomial set is invariant under a group action, we construct a set of invariants that define the same variety. Our construction can be seen as a generalization of the previously known construction for finite groups. The result though has to be understood outside an invariant variety which is independent of the polynomial set considered. We introduce the *symmetrizations* of a polynomial that are polynomials in a generating set of rational invariants. The generating set of rational invariants and the symmetrizations are constructed w.r.t. a section to the orbits of the group action.

Keywords: Rational invariants; Polynomial systems with symmetry; Section in invariant theory.

1 Introduction

Consider the variety \mathcal{F} in \mathbb{C}^n of a finite set of polynomials F in $\mathbb{C}[z_1, \dots, z_n]$. \mathcal{F} can be invariant under the action of a group \mathcal{G} without the polynomials in F being themselves invariant. For a given set F of polynomials as above we shall determine a set of invariant functions \tilde{F} such that the zero set of \tilde{F} is equal to the variety of F outside of some proper subvariety \mathcal{W} . The elements of \tilde{F} are polynomials in a fixed finite set of generating rational invariants. The restriction to a dense open set is therefore unavoidable for a general statement. Yet this dense open set is independent of F .

When \mathcal{G} is a finite group acting regularly, a system of polynomial invariants \tilde{F} that have the same variety as F can be determined explicitly. The construction of \tilde{F} can be found for instance in the proof of [28, Proposition 2.6.4] and this construction also applies for \mathcal{G} -invariant semi-algebraic sets [3]. The existence of such a \tilde{F} for a compact group is proved in [2]. It was nonetheless an open question in [3] whether there exists a constructive approach. The present article aims to provide such a construction for rational actions of any algebraic group.

A polynomial system that does not exhibit the symmetry of its variety can for instance appear as the result of algebraic computations as these rarely preserve the known symmetry of the problem. Determining an equivalent system in terms of a generating set of invariants allows further qualitative analysis and a simplified resolution. Specific methods address the resolution of a polynomial system given by the components of an equivariant map [10]. When the group action is given by orthogonal representations one can construct a set of polynomial invariants with the same variety over the reals [9, 16, 30]. Yet, even in the equivariant case, there is no systematic process to produce a system of invariants with the same set of zeros in general.

The construction of the set \tilde{F} above is based on a concept of *symmetrizations* of a polynomial. This latter builds on the construction of the field of rational invariants that makes central use of the notion of section to the orbits. The related construction in [11] was later extended to the construction of the ring of polynomial invariants of some non reductive groups [7, Section 4.10]. We revisit here this construction with a notion of section less restrictive than the *cross section* used in [11]. The geometric interpretation of the constructive

*INRIA Méditerranée, 06902 Sophia Antipolis, France. evelyne.hubert@inria.fr

definition of symmetrization allows us to use an argument analogous to the finite group case to prove that the zero set of the symmetrizations \tilde{F} of the elements of F is equal to the variety of F . Yet the statement in this case has to be understood outside of a proper invariant subvariety \mathcal{W} . The latter depends on the group action and the chosen section but also the term order with which the generating set of invariants is produced.

The symmetrizations we introduce are connected to the concept of algebraic invariantization in [12]. The latter was introduced as a constructive approach to the local invariantization process associated to the moving frame construction of differential invariants and invariant derivations [8]. One can also see that the treatment of polynomial systems under a scaling symmetry (in particular multi-homogeneous polynomial systems) in [13] is a special case of symmetrization.

In the next section we define the group actions to be considered as well as the notion of *section of degree e* to the orbits. We show how to compute a finite set of generating rational invariants. They are the coefficients of a reduced Gröbner basis of the *orbit-section* ideal. In Section 3 we give a constructive definition of symmetrization w.r.t. a given section to the orbits: to any polynomial f is associated e *symmetrizations*, where e is the degree of the section to the orbits. These symmetrizations are polynomials in the generating invariants. If F is a set of polynomials whose variety is invariant under the group action then the set \tilde{F} of the symmetrizations of the elements of F have the same zero set. The result has to be understood within a \mathcal{G} -invariant open set where the reduced Gröbner basis of the orbit-section ideal specializes well.

Acknowledgments: The authors is grateful to Guillaume Moroz and Fabrice Rouillier for discussions on the specialisation properties of Gröbner bases.

2 Construction of rational invariants

We shall first introduce the notions and notations to be used in the article. We then present an algorithm to compute generating sets of invariants endowed with rewrite rules. For that we introduce a definition of section to the orbits of the group action less restrictive than the cross section of [11] and provide a simplified set of proofs. Theorem 2.4 and 2.6 can nonetheless be compared respectively with [11, Theorem 3.5 and 3.7]. The different notions of sections are discussed in the last subsection.

2.1 Rational action of an algebraic group

\mathbb{K} is a field of characteristic zero, $\overline{\mathbb{K}}$ is an algebraically closed field extension of \mathbb{K} . The groups we consider are affine algebraic groups. They are given by an affine algebraic variety \mathcal{G} endowed with a group operation $\cdot : \mathcal{G} \times \mathcal{G} \rightarrow \mathcal{G}$ and an inverse $\mathcal{G} \rightarrow \mathcal{G}$ given by regular maps. To be explicit, we assume that \mathcal{G} is embedded in $\overline{\mathbb{K}}^l$ and $G \subset \mathbb{K}[\lambda_1, \dots, \lambda_l]$ is its defining ideal. The coordinate ring $\mathbb{K}[\mathcal{G}]$ can be identified with the quotient algebra $\mathbb{K}[\lambda_1, \dots, \lambda_l]/G$.

A rational action of \mathcal{G} on an affine space $\mathcal{Z} = \overline{\mathbb{K}}^n$ is defined by a homomorphism ρ from \mathcal{G} to the group of birational maps of \mathcal{Z} . In practice it is given by a rational map $\mathcal{G} \times \mathcal{Z} \rightarrow \mathcal{Z}$, $(\lambda, z) \mapsto \lambda \star z = \rho(\lambda)(z)$ defined by quotients of polynomials:

$$\lambda \star z = \left(\frac{h_1(\lambda, z)}{h_0(\lambda, z)}, \dots, \frac{h_n(\lambda, z)}{h_0(\lambda, z)} \right)$$

where $h_0, h_1, \dots, h_n \in \mathbb{K}[\lambda_1, \dots, \lambda_l, z_1, \dots, z_n]$. When we write $(\bar{\lambda}, \bar{z}) \in \mathcal{G} \times \mathcal{Z}$ we mean that $(\bar{\lambda}, \bar{z})$ belongs to the open set of $\mathcal{G} \times \mathcal{Z}$ where $\bar{\lambda} \star \bar{z}$ is well defined.

A rational action of \mathcal{G} on \mathcal{Z} induces an action on the field of rational functions $\mathbb{K}(z) = \mathbb{K}(z_1, \dots, z_n)$ given by $(\lambda \star f)(z) = f(\lambda^{-1} \star z)$. The set of rational invariants $\mathbb{K}(z)^{\mathcal{G}}$ is the subfield of $\mathbb{K}(z)$ of rational functions f s.t. $\lambda \star f = f$, for all $\lambda \in \mathcal{G}$. As such, $\mathbb{K}(z)^{\mathcal{G}}$ is finitely generated (cf. for instance [15, Theorem 24.9]).

The orbit $\mathcal{O}_{\bar{z}}$ of $\bar{z} \in \mathcal{Z}$ is the image of the rational map $\mathcal{G} \rightarrow \mathcal{Z}$, $\bar{\lambda} \mapsto \bar{\lambda} \star \bar{z}$. The (Zariski) closure of $\mathcal{O}_{\bar{z}}$ is thus the variety of the elimination ideal (see for instance [1, Theorem 7.69], [4, Chapter 3])

$$\mathcal{O}_{\bar{z}} = (G + (h_0(\lambda, \bar{z})\mathfrak{z}_1 - h_1(\lambda, \bar{z}), \dots, h_0(\lambda, \bar{z})\mathfrak{z}_n - h_n(\lambda, \bar{z}))) : h_0^\infty \cap \overline{\mathbb{K}[\mathfrak{z}, \lambda]}.$$

In the above, we have introduced a new set of variables $\mathfrak{z} = \{\mathfrak{z}_1, \dots, \mathfrak{z}_n\}$. A root $\bar{\mathfrak{z}} \in \mathcal{Z}$ of the ideal $\mathcal{O}_{\bar{z}}$ belongs to the closure of the orbit $\mathcal{O}_{\bar{z}}$ of \bar{z} . We shall pursue with this additional set of variables all along this paper.

We shall work mostly with $\mathbb{K}(z)[\mathfrak{z}] = \mathbb{K}(z_1, \dots, z_n)[\mathfrak{z}_1, \dots, \mathfrak{z}_n]$. Consider the ideal O of $\mathbb{K}(z)[\mathfrak{z}]$ defined as the elimination ideal:

$$O = (G + (h_0(\lambda, z)\mathfrak{z}_1 - h_1(\lambda, z), \dots, h_0(\lambda, z)\mathfrak{z}_n - h_n(\lambda, z))) : h_0^\infty \cap \mathbb{K}(z)[\mathfrak{z}, \lambda].$$

For a given term order on \mathfrak{z} , the reduced Gröbner basis B of O can be computed by elimination [1, Chapter 6.2] [5, Chapter 3]. One proves that the coefficient of B form a generating set of rational invariants [23], [11, Theorem 2.14].

An alternative construction presented in [11, Section 3] produces a more usable output. It makes use of a *cross-section* to the orbit. We introduce next the less demanding notion of *section to the orbits* and revise accordingly the construction of a generating set of rational invariants in Section 2.3.

2.2 Sections to the orbits

After defining *sections to the orbits of a group action*, we provide an algebraic characterisation of these. The difference with the *cross-sections* used in [11] is discussed in Section 2.4.

Definition 2.1 *For a given rational action of \mathcal{G} on \mathcal{Z} , an irreducible variety \mathcal{P} is a section of degree e to the orbits if there exists an open dense subset \mathcal{U} of \mathcal{Z} such that the orbit of any point $\bar{z} \in \mathcal{U}$ intersects \mathcal{P} at e points, counted with multiplicities.*

Thus a section cannot be contained in a proper \mathcal{G} -invariant subvariety of \mathcal{Z} . If the generic orbits are of dimension d , a section is of codimension d . One can always choose an affine linear space as a section [11, Theorem 3.3], or even the level set of some of the coordinate functions [12, Theorem 1.6]. For generic affine linear space of codimension d the degree of the section it defines is the degree of the orbits. Sections of lower degree can be obtained by taking into consideration the points at infinity or the singular points of the closure of generic orbits, as illustrated in Example 2.3. Section of degree one are of particular interest, as we shall point out at several places.

We shall express the condition for the orbits of an open dense set of points in \mathcal{Z} to intersect \mathcal{P} in e points. As before, a point $\bar{z} \in \mathcal{Z}$ is represented by the variables (z_1, \dots, z_n) . We introduce the variables $(\mathfrak{z}_1, \dots, \mathfrak{z}_n)$ in order to express the condition that a different point $\bar{\mathfrak{z}} \in \mathcal{Z}$ belongs to $\mathcal{O}_{\bar{z}}$ and to \mathcal{P} . A section \mathcal{P} is determined by a prime ideal P of codimension d that we take in $\mathbb{K}[\mathfrak{z}] = \mathbb{K}[\mathfrak{z}_1, \dots, \mathfrak{z}_n]$.

Proposition 2.2 *Assume the generic orbits have dimension d and take $P \subset \mathbb{K}[\mathfrak{z}_1, \dots, \mathfrak{z}_n]$ as a prime ideal of codimension d . Consider*

$$A = (h_0(\lambda, z)\mathfrak{z}_1 - h_1(\lambda, z), \dots, h_0(\lambda, z)\mathfrak{z}_n - h_n(\lambda, z)) \subset \mathbb{K}(z)[\mathfrak{z}, \lambda] \quad (1)$$

Then the variety \mathcal{P} of the prime ideal $P \subset \mathbb{K}[\mathfrak{z}]$ is a section if the ideal

$$I_{\mathcal{P}} = (G + A + P) : h_0^\infty \cap \mathbb{K}(z)[\mathfrak{z}] \quad (2)$$

is zero dimensional. The dimension e of the quotient algebra $\mathbb{K}(z)[\mathfrak{z}]/I_{\mathcal{P}}$ as a $\mathbb{K}(z)$ -vector space is the degree of the section.

PROOF: Consider $A_{\bar{z}} = (h_0(\lambda, \bar{z})\mathfrak{z}_1 - h_1(\lambda, \bar{z}), \dots, h_0(\lambda, \bar{z})\mathfrak{z}_n - h_n(\lambda, \bar{z})) \subset \overline{\mathbb{K}}[\mathfrak{z}, \lambda]$. The ideal $I_{\bar{z}} = (G + A_{\bar{z}} + P) : h_0^\infty \cap \mathbb{K}[\mathfrak{z}]$ is an ideal whose variety is the Zarisky closure of $\mathcal{O}_{\bar{z}} \cap \mathcal{P}$.

For a given term order on \mathfrak{z} , the reduced Gröbner basis B for $I_{\mathcal{P}}$ can be computed by elimination [1, Chapter 6.2], [5, Chapter 3]. [1, Theorem 6.54] or [5, Chapter 5.3 Theorem 6] provide a criterion for $I_{\mathcal{P}}$ to be zero dimensional. The dimension e of $\mathbb{K}(z)[\mathfrak{z}]/I_{\mathcal{P}}$ can be deduced from the leading terms B according to [1, Theorem 6.54] or [5, Chapter 5.3 Proposition 4].

One can determine [5, Chapter 6.3 Proposition 1] an hypersurface \mathcal{W} such that for any $\bar{z} \in \mathcal{Z} \setminus \mathcal{W}$ the reduced Gröbner basis of $I_{\bar{z}}$ is obtained by taking the specialization $B_{\bar{z}}$ of B under $z \mapsto \bar{z}$. In particular, for $\bar{z} \in \mathcal{Z} \setminus \mathcal{W}$, $B_{\bar{z}}$ has the same leading terms as B . Thus $I_{\bar{z}}$ is zero dimensional if $I_{\mathcal{P}}$ is zero dimensional. Furthermore then, the dimension of $\mathbb{K}[\mathfrak{z}]/I_{\bar{z}}$ is e so that the variety of $I_{\bar{z}}$ consists of e points (counted with multiplicities) [4, Chapter 4.2 Corollary 2.5]. Thus $\mathcal{O}_{\bar{z}} \cap \mathcal{P}$ consists of e points, counted with multiplicity. \square

The proof above provides an algorithmic characterisation for P to define a section. Let B be the reduced Gröbner basis (according to any term order) of $I_{\mathcal{P}}$. P defines a section of degree e if the normal set of monomials w.r.t. B [1, Chapter 6.3] (*i.e.* the complementary set to the leading terms of $I_{\mathcal{P}}$ [5, Chapter 5.3]) has finite cardinal e . As we shall see in next section, the reduced Gröbner bases of $I_{\mathcal{P}}$ also delivers a generating set of rational invariants for the action.

Example 2.3 SCALINGS IN THE PLANE. Consider the action of the multiplicative group \mathbb{K}^* given by

$$\begin{aligned} \star : \mathbb{K}^* \times \mathbb{K}^2 &\rightarrow \mathbb{K}^2 \\ (\lambda, (x, y)) &\mapsto (\lambda^a x, \lambda^b y) \end{aligned}$$

where a and b are positive integers that we assume here relatively prime. The ideal of the closure of the orbit of $(\bar{x}, \bar{y}) \in \overline{\mathbb{K}}^2 \setminus \{(0, 0)\}$ is then given by

$$O_{(\bar{x}, \bar{y})} = (x^b \eta^a - y^a \mathfrak{x}^b) \subset \overline{\mathbb{K}}[\mathfrak{x}, \eta].$$

As a side note we shall observe that the origin is in the closure of all the orbits. There is therefore no non constant polynomial invariant for this action [7, Lemma 2.4.5]. While rational invariants always separate orbits of points outside of a proper closed set (here the variety of the polynomial xy), polynomial invariants provide no separation for the scalings considered here.

A generic affine line in $\overline{\mathbb{K}}^2$ is a section of degree $\max(a, b)$. But $P = (\mathfrak{x} - 1) \in \mathbb{K}[\mathfrak{x}, \eta]$ defines a section of degree a since the ideal of the intersection of the orbit of $(x, y) \in \overline{\mathbb{K}}^2 \setminus \{(0, t) \mid t \in \overline{\mathbb{K}}\}$ with the variety \mathcal{P} of P is

$$I_{\mathcal{P}} = \left(\mathfrak{x} - 1, \eta^a - \frac{y^a}{x^b} \right).$$

Alternatively a section of degree 1 is provided by the Bezout coefficients $\alpha, \beta \in \mathbb{Z}$ s.t. $\alpha a - \beta b = 1$. For the purpose of this example we can assume that $\alpha, \beta \in \mathbb{N}$. If we choose $P = (\mathfrak{x}^\alpha - \eta^\beta)$ then the ideal of the intersection of the orbit of $(x, y) \in \overline{\mathbb{K}}^2 \setminus \{(0, y) \mid y \in \overline{\mathbb{K}}\}$ with the variety \mathcal{P} of P is

$$I_{\mathcal{P}} = \left(\mathfrak{x} - \left(\frac{y^a}{x^b} \right)^\beta, \eta - \left(\frac{y^a}{x^b} \right)^\alpha \right).$$

This generalizes for scalings in any dimension, *i.e.* diagonal linear actions of the algebraic torus $(\mathbb{K}^*)^d$: we can compute the (binomial) equations of a section of degree one with linear algebra over the integers [13, 14].

2.3 Generating invariants and rewriting

As can be observed in the examples presented above, the coefficients of the reduced Gröbner basis of the orbit-section ideal $I_{\mathcal{P}}$ are rational invariants. The reason is that $\mathcal{O}_{\bar{z}} = \mathcal{O}_{\lambda \star \bar{z}}$ and therefore $\mathcal{O}_{\bar{z}} \cap \mathcal{P} = \mathcal{O}_{\lambda \star \bar{z}} \cap \mathcal{P}$

so that a canonical representation of the orbit-section ideal $I_{\mathcal{P}}$ must be defined over $\mathbb{K}(z)^{\mathcal{G}}$. A reduced Gröbner basis is such a canonical representative. We furthermore show that a reduced Gröbner basis allows to rewrite any invariants in terms of its coefficients.

Theorem 2.4 *Consider a term order on the variables $\mathfrak{z}_1, \dots, \mathfrak{z}_n$. The coefficients of the reduced Gröbner basis of the orbit-section ideal $I_{\mathcal{P}}$ in $\mathbb{K}(z)[\mathfrak{z}]$ belong to $\mathbb{K}(z)^{\mathcal{G}}$.*

PROOF: For a given term order, the reduced Gröbner basis of an ideal is unique [1, Theorem 5.3], [5, Chapter 2.7 Definition 4 and Theorem 5]. Let B be the reduced Gröbner basis for $I_{\mathcal{P}}$ for the given term order on \mathfrak{z} . As such it consists of monic polynomials in $\mathbb{K}(z)[\mathfrak{z}]$.

There is a closed proper subset \mathcal{W} of \mathcal{Z} s.t. for $\bar{z} \in \mathcal{Z} \setminus \mathcal{W}$ the image $B_{\bar{z}}$ of B under specialization $z \mapsto \bar{z}$ is the reduced Gröbner basis for the ideal $I_{\bar{z}} = (G + A_{\bar{z}} + P) : h_0^{\infty} \cap \overline{\mathbb{K}[\mathfrak{z}]}$ [5, Chapter 6.3 Proposition 1]. As $\mathcal{O}_{\bar{z}} \cap \mathcal{P}$ is zero dimensional, it is the variety of $I_{\bar{z}}$.

Since $\mathcal{O}_{\bar{z}} = \mathcal{O}_{\bar{\lambda} \star \bar{z}}$ and thus $\mathcal{O}_{\bar{z}} \cap \mathcal{P} = \mathcal{O}_{\bar{\lambda} \star \bar{z}} \cap \mathcal{P}$, for $\bar{z} \in \mathcal{Z} \setminus \mathcal{W}$ and $\bar{\lambda} \in \mathcal{G}$, the specializations of B to \bar{z} and to $\bar{\lambda} \star \bar{z}$ brings the same reduced Gröbner basis. Therefore $B \subset \mathbb{K}(z)^{\mathcal{G}}[\mathfrak{z}]$. \square

In this construction it is clear that the coefficients of the Gröbner basis of $I_{\mathcal{P}}$ *separate* generic orbits. According to [27, Theorem 2] or [26, Lemma 2.1], we can deduce that they form a generating set. The alternative proof we give next is constructive. We show how to rewrite any invariant in terms of the coefficients of the reduced Gröbner basis. This is similar to [11, Theorem 3.7]. The following property of rational invariants is necessary in the proof of Theorem 2.6.

Lemma 2.5 *If p/q is a rational invariant, with $p, q \in \mathbb{K}[z]$ relatively prime, then the varieties $\mathcal{V}(p)$ and $\mathcal{V}(q)$ are invariant under the action of \mathcal{G} .*

PROOF: By hypothesis $p(z)q(\lambda \star z) = q(z)p(\lambda \star z)$ for all $(\lambda, z) \in \mathcal{G} \times \mathcal{Z}$. Hence $p(\lambda \star z) = 0$ for all $(\lambda, z) \in \mathcal{G} \times (\mathcal{V}(p) \setminus \mathcal{V}(q))$. Since p and q are relatively prime, $\mathcal{V}(p) \setminus \mathcal{V}(q)$ is dense in $\mathcal{V}(p)$. Hence $p(\lambda \star z)$ has to vanish on the whole of $\mathcal{G} \times \mathcal{V}(p)$. \square

As a side note, we shall remark that when \mathcal{G} is connected and acts regularly on \mathcal{Z} , one can furthermore conclude that p and q are *semi-invariants* with the same *weight*, i.e. $p(\lambda \star z) = \chi(\lambda)p(z)$ and $q(\lambda \star z) = \chi(\lambda)q(z)$ where $\chi : \mathcal{G} \rightarrow \overline{\mathbb{K}}^*$ is a group morphism [26, Theorem 3.1 and 3.3].

Theorem 2.6 *Consider a term order on the variables \mathfrak{z} . Let $\{r_1, \dots, r_m\} \in \mathbb{K}(z)^{\mathcal{G}}$ be the coefficients of the reduced Gröbner basis B of $I_{\mathcal{P}}$. Then $\mathbb{K}(z)^{\mathcal{G}} = \mathbb{K}(r_1, \dots, r_m)$ and we can rewrite any rational invariant $\frac{p}{q}$, with $p, q \in \mathbb{K}[z]$ relatively prime, in terms of those as follows.*

Take a new set of indeterminates $\mathfrak{r}_1, \dots, \mathfrak{r}_m$ and consider the set $\mathfrak{B} \subset \mathbb{K}[\mathfrak{r}, \mathfrak{z}]$ obtained from B by substituting r_i by \mathfrak{r}_i . Let $a(\mathfrak{r}, \mathfrak{z}) = \sum_{\alpha \in \mathbb{N}^n} a_{\alpha}(\mathfrak{r})\mathfrak{z}^{\alpha}$ and $b(\mathfrak{r}, \mathfrak{z}) = \sum_{\alpha \in \mathbb{N}^n} b_{\alpha}(\mathfrak{r})\mathfrak{z}^{\alpha}$ in $\mathbb{K}[\mathfrak{r}, \mathfrak{z}]$ be the normal forms¹ of $p(\mathfrak{z})$ and $q(\mathfrak{z})$ w.r.t. \mathfrak{B} . There exists $\alpha \in \mathbb{N}^m$ s.t. $b_{\alpha}(\mathfrak{r}) \neq 0$ and for any such α we have $\frac{p(\mathfrak{z})}{q(\mathfrak{z})} = \frac{a_{\alpha}(\mathfrak{r})}{b_{\alpha}(\mathfrak{r})}$.

PROOF: We first note that neither $q(\mathfrak{z})$, nor $p(\mathfrak{z})$, belong to P . Indeed the orbits of the points on \mathcal{P} fill an open dense set of \mathcal{Z} by hypothesis. Since $\mathcal{V}(q)$ invariant (Lemma 2.5), $\mathcal{P} \subset \mathcal{V}(q)$ would imply $q = 0$.

We now argue that $I_{\mathcal{P}} \cap \mathbb{K}[\mathfrak{z}] = P$. We obviously have $P \subset I_{\mathcal{P}} \cap \mathbb{K}[\mathfrak{z}]$ and therefore the projection of $\mathcal{V}(I_{\mathcal{P}} \cap \mathbb{K}[\mathfrak{z}])$ on the \mathfrak{z} -components is included in \mathcal{P} . Conversely, for a generic point \mathfrak{z} on \mathcal{P} , the points $(\lambda \star \mathfrak{z}, \mathfrak{z})$, for $\lambda \in \mathcal{G}$ lies in $\mathcal{V}(I_{\mathcal{P}} \cap \mathbb{K}[\mathfrak{z}, \mathfrak{z}])$. The projection of this latter on the second component is thus dense in \mathcal{P} .

¹For the reductions in $\mathbb{K}[\mathfrak{r}, \mathfrak{z}]$ the term order on \mathfrak{z} is extended to a block order $\mathfrak{r} \ll \mathfrak{z}$ so that the set of leading terms of \mathfrak{B} is equal to the set of leading terms of B .

Therefore neither $p(\mathfrak{z})$ nor $q(\mathfrak{z})$ belong to $I_{\mathcal{P}}$. The normal forms of $q(\mathfrak{z})$ and $p(\mathfrak{z})$ w.r.t. B are, respectively, $b(r, \mathfrak{z})$ and $a(r, \mathfrak{z})$ and they are thus both different from zero.

Since p/q is invariant, $p(z)q(\lambda \star z) \equiv q(z)p(\lambda \star z) \pmod{G}$. Hence $p(z)q(\mathfrak{z}) - q(z)p(\mathfrak{z})$ belongs to $I_{\mathcal{P}}$ so that its normal form with respect to B must be zero: $p(z)b(r, \mathfrak{z}) = q(z)a(r, \mathfrak{z})$. The conclusion follows. \square

Theorem 2.6 applies in particular to polynomial invariants. We immediately see that:

Corollary 2.7 *Any polynomial invariant can be written as a polynomial in $\{r_1, \dots, r_m\}$.*

Therefore a case of special interest is when the coefficients of the reduced Gröbner basis have no denominators.

Proposition 2.8 *If the coefficients of a reduced Gröbner basis of $I_{\mathcal{P}}$ are polynomials, i.e. belong to $\mathbb{K}[z]$, then they generate the ring of polynomial invariants $\mathbb{K}[z]^{\mathcal{G}}$.*

Example 2.9 *Consider the linear action of SO_2 on $\mathcal{Z} = \overline{\mathbb{K}}^3$ acting by rotation on the (x, y) -plane. We have*

$$G = (\lambda^2 + \mu^2 - 1) \subset \mathbb{K}[\lambda, \mu] \quad \text{and} \quad A = (\mathfrak{x} - (\lambda x - \mu y), \mathfrak{y} - (\mu x + \lambda y), \mathfrak{z} - z) \subset \mathbb{K}(x, y, z)[\lambda, \mu, \mathfrak{x}, \mathfrak{y}, \mathfrak{z}].$$

Choose the section \mathcal{P} of degree 2 given by $P = (\mathfrak{x})$. Then $I_{\mathcal{P}} = (\mathfrak{x}, \mathfrak{y}^2 - (x^2 + y^2), \mathfrak{z} - z)$. Thus $r = x^2 + y^2$ and z form a generating set for $\mathbb{K}(x, y, z)^{\mathcal{G}}$, but also for $\mathbb{K}[x, y, z]^{\mathcal{G}}$.

More generally, when the coefficients are the quotients of invariant polynomials, they provide generators for a localization of the invariant ring. The generators of the invariant ring can then be computed following [7, Section 4.1.2].

Section of degree one are of special interest. For these, the reduced Gröbner basis of the orbit-section ideal $I_{\mathcal{P}}$, w.r.t. any term order, is of the form $\{\mathfrak{z}_1 - r_1(z), \dots, \mathfrak{z}_n - r_n(z)\}$, where $r_i \in \mathbb{K}(z)^{\mathcal{G}}$. The rewriting described in Theorem 2.6 is then a simple substitution: if f is a rational invariant then $f(z_1, \dots, z_n) = f(r_1(z), \dots, r_n(z))$.

Example 2.10 *Following up on Example 2.3, for any invariant $f \in \mathbb{K}(z)^{\mathcal{G}}$ we have $f(x, y) = f(r^{\beta}, r^{\alpha})$, where $r = \frac{y^{\alpha}}{x^{\beta}}$.*

2.4 Section, quasi-section, cross-section, partial section

Different notions of *sections* to the orbits of a group action appear in invariant theory to show properties of the field of invariants [25, 26]. The present concept of *section of degree e* appears as *quasi-section* in [26], without specifying the degree. Only section of degree 1 are referred there as *section*, and sometimes as *rational section*.

In the course of providing an algebraic formulation of the *moving frame* construction of differential invariants [8, 12], the concept of *cross-section of degree e* was introduced and applied to compute a generating set of invariants in [11], providing a more efficient alternative to the earlier constructions (overviewed in [11, Section 2.3]). As explained next, *cross-sections of degree e* differ slightly from the present *section of degree e*

In [11, Definition 3.1] an irreducible ideal P , of complementary dimension to the generic orbits, defines a cross-section if the ideal $O + P$ is zero-dimensional and radical, where $O = (G + A) : h_0^{\infty} \cap \mathbb{K}(z)[\mathfrak{z}]$ is the ideal of the generic orbit. The degree of the cross-section is then the dimension of the $\mathbb{K}(z)$ -vector space $\mathbb{K}(z)[\mathfrak{z}]/(O + P)$. This is the number of points of intersection of the closure of a generic orbit with the variety \mathcal{P} of P . The following example shows how this can differ from the present notion of section.

Example 2.11 *Consider the scaling $\lambda \star (x, y) = (\lambda^2 x, \lambda^3 y)$ and \mathcal{P} as the variety of $P = (\mathfrak{y} - \mathfrak{x}) \subset \mathbb{K}[\mathfrak{x}, \mathfrak{y}]$. On one hand, the orbit-section ideal is*

$$I_{\mathcal{P}} = \left(\mathfrak{y} - \frac{x^3}{y^2}, \mathfrak{x} - \frac{x^3}{y^2} \right)$$

so that \mathcal{P} is a section of degree one. On the other hand $O = (y^2\mathfrak{x}^3 - x^3\mathfrak{y}^2)$ so that

$$O + P = \left(\mathfrak{x} - \mathfrak{y}, \mathfrak{y}^2 \left(\mathfrak{y} - \frac{x^3}{y^2} \right) \right).$$

The closure of the generic orbit contains the origin, as does \mathcal{P} . \mathcal{P} fails to be a cross-section because $O + P$ is not radical.

Both concepts lead to valid constructions for the fields of rational invariants. The present concept of section appears nonetheless as more favorable. For instance, sections of degree one can be obtained for any scaling, i.e. diagonal representation of tori [13, 14]. As shown in the previous example, this is no longer true for cross-sections.

Analogues to Theorem 2.4 and 2.6 were proved in [11, 23] for the orbit ideal $O = (G + A) : h_0^\infty$ and it is natural to consider intermediate cases where \mathcal{P} is of lower dimension than the codimension of the generic orbits. The ideal $(G + A + P) : h_0^\infty$ is not zero dimensional then. The proofs of Theorem 2.4 and 2.6 used the following properties:

- \mathcal{P} is not contained in any invariant hypersurface
- $(G + A + P) : h_0^\infty \cap \mathbb{K}[\mathfrak{z}] = P$.

Those properties would be sufficient to define a notion of *partial section* and this line of ideas was molded in the terminology of *extended Derksen ideals* in [7, Section 4.10], de-emphasizing the geometrical significance.

3 Symmetrization

We shall define a concept of symmetrization with respect to a section. The definition is constructive. We then prove that within a \mathcal{G} -invariant open set, which depends on the chosen section and a term order, the symmetrization of a polynomial system produces invariants with the same variety. This \mathcal{G} -invariant open set is given as the locus of points with good specialisation properties of the reduced Gröbner basis of the orbit-section ideal. We discuss how to determine this locus first.

3.1 The singular set \mathcal{W}

In Section 2 we have made use of a reduced Gröbner basis B of the orbit-section ideal $I_{\mathcal{P}}$ in $\mathbb{K}(z)[\mathfrak{z}]$ to determine a generating set of $\mathbb{K}(z)^{\mathcal{G}}$ (Theorem 2.6). In the proofs we have used the fact that there exists a variety \mathcal{W} such that for $\bar{z} \in \mathcal{Z} \setminus \mathcal{W}$ the specialisation $B_{\bar{z}}$ of B is a reduced Gröbner basis of the ideal of $\mathcal{O}_{\bar{z}} \cap \mathcal{P}$, the intersection of the orbit of \bar{z} with the section \mathcal{P} .

In this section we make more precise how to determine a relevant \mathcal{W} . We shall first refine a relatively simple specialisation criterion given as [17, Theorem 4.3], that can also be found as [5, Chapter 5.3 Proposition 1]. The Gröbner cover introduced in [29] made algorithmic in [19] provides a sharper \mathcal{W} .

Proposition 3.1 *Consider a block term order on $\mathbb{K}[z, \mathfrak{z}, \lambda]$ where $z < \mathfrak{z} < \lambda$. Let \hat{B} be the reduced Gröbner basis of $(G + A + P) : h_0^\infty$ where $G \subset \mathbb{K}[\lambda]$ is the ideal of the group \mathcal{G} ,*

$$A = ((h_0(\lambda, z)_{\mathfrak{z}1} - h_1(\lambda, z), \dots, h_0(\lambda, z)_{\mathfrak{z}n} - h_n(\lambda, z)) \subset \mathbb{K}[z, \lambda, \mathfrak{z}]$$

and $P \subset \mathbb{K}[\mathfrak{z}]$ is the ideal of the section.

\hat{B} is a Gröbner basis for $(G + A + P) : h_0^\infty$ considered in $\mathbb{K}(z)[\mathfrak{z}, \lambda]$ with the restricted term order on \mathfrak{z} and λ . Let \bar{B} be its reduced part and $B = \bar{B} \cap \mathbb{K}(z)[\mathfrak{z}]$. Then B is the reduced Gröbner basis of $I_{\mathcal{P}}$ for the term order on \mathfrak{z} .

Let $a \in \mathbb{K}[z]$ be the product of the leading coefficients of the elements of \hat{B} considered as polynomials in \mathfrak{z} and λ with the restricted term order. Define \mathcal{W} to be the maximal \mathcal{G} -invariant subset of the variety of a .

For any $\bar{z} \in \mathcal{Z} \setminus \mathcal{W}$, the specialisation $B_{\bar{z}}$ of B at $z \mapsto \bar{z}$ is the Gröbner basis for the ideal of $\mathcal{O}_{\bar{z}} \cap \mathcal{P}$, the intersection of the orbit of \bar{z} with the section.

PROOF: Let \mathcal{U} be the variety of a . Then [5, Chapter 5.3 Proposition 1] implies that for $\bar{z} \in \mathcal{Z} \setminus \mathcal{U}$, $B_{\bar{z}}$ is the reduced Gröbner basis of the ideal of $\mathcal{O}_{\bar{z}} \cap \mathcal{P}$.

If $\bar{z} \in \mathcal{U} \setminus \mathcal{W}$ there exists $\bar{\lambda} \in \mathcal{G}$ such that $\bar{\lambda} \star \bar{z} \notin \mathcal{U}$. Hence the specialization $B_{\bar{\lambda} \star \bar{z}}$ is the Gröbner basis of $\mathcal{O}_{\bar{\lambda} \star \bar{z}} \cap \mathcal{P} = \mathcal{O}_{\bar{z}} \cap \mathcal{P}$ and we have $B_{\bar{\lambda} \star \bar{z}} = B_{\bar{z}}$. \square

As we shall see in the examples below, the variety \mathcal{W} obtained this way is not minimal. To simplify the exposition, we shall speak of the *singular set* of B to be exact set of points \bar{z} where the specialisation $B_{\bar{z}}$ is either ill defined or does not form the reduced Gröbner bases of $(G + A_{\bar{z}} + P) : \bar{h}_0^\infty \cap \mathbb{K}[\mathfrak{z}]$. Similarly for \bar{B} .

In [29] it is shown that the set of points \bar{z} where \bar{B} specializes well is *parametric* [19, Definition 4]. In the present case, this means that the singular set of \bar{B} is an algebraic variety \mathcal{W} . The first component of the *canonical Gröbner cover*, that can be computed thanks to the algorithm presented [19], provides generators for the ideal W of \mathcal{W} . By the argument given in the proof of the proposition above, the singular set for B is \mathcal{G} -invariant. It might be a proper subset of the singular set of \bar{B} , as illustrated in Example 3.4. To obtain the singular set for B , one needs to recombine the components of the canonical Gröbner cover with the subalgorithms *LCUnion* and *Combine* presented in [19].

Example 3.2 Consider the action of $\mathcal{G} = \overline{\mathbb{K}}^*$ on the plane given by $\lambda \star (x, y) = (\lambda^{-1}x, \lambda y)$. We have $G = (\lambda\mu - 1)$ in $\mathbb{K}[\lambda, \mu]$, $A = (\mathfrak{x} - \mu x \mathfrak{y} - \lambda y) \subset \mathbb{K}(x, y)[\mathfrak{x}, \mathfrak{y}, \lambda, \mu]$ and let us take the section defined by $P = (\mathfrak{x} - 1) \subset \mathbb{K}[\mathfrak{x}, \mathfrak{y}]$.

The reduced Gröbner basis of $(G + A + P)$ in $\mathbb{K}[x, y, \mathfrak{x}, \mathfrak{y}, \lambda, \mu]$ is $\hat{B} = \{\mathfrak{x} - 1, \mathfrak{y} - xy, \lambda - x, x\mu - 1\}$ so that $a = x$. Its variety $\mathcal{V}(x)$ is invariant. This corroborates the fact that the orbit of the points $(0, \bar{y})$ do not intersect the section defined by P . Hence $\mathcal{W} = \mathcal{V}(x)$ is the singular set of $B = \{\mathfrak{x} - 1, \mathfrak{y} - xy\}$.

Consider now the action given by $\lambda \star (x, y) = (\lambda x, \lambda y)$. We have

$$\hat{B} = \{\mathfrak{x} - 1, x\mathfrak{y} - y, x\lambda - 1, y\lambda - \mathfrak{y}, \mu - x\}$$

so that $a = xy$. Its variety $\mathcal{W} = \mathcal{V}(x) \cup \mathcal{V}(y)$ is invariant.

The reduced Gröbner basis of $I_{\mathcal{P}}$ is $B = \{\mathfrak{x} - 1, \mathfrak{y} - \frac{y}{x}\}$. It is apparent that the specialisation at the points $(\bar{x}, \bar{y}) = (0, \bar{y})$ is ill defined and indeed the orbits of these points do not intersect the section \mathcal{P} . On the other hand the specialisation at $(\bar{x}, 0)$, with $\bar{x} \neq 0$, does provide the Gröbner basis for the ideal of $\mathcal{O}_{(\bar{x}, 0)} \cap \mathcal{P}$.

When computing the canonical Gröbner cover with the algorithm described in [19, 20] and implemented in SINGULAR [6] one ascertains that the singular set of \bar{B} is actually $\mathcal{V}(x)$.

Example 3.3 Following on Example 2.9. Here

$$\hat{B} = \{\mathfrak{x}, \mathfrak{y}^2 + 1 - (y^2 + x^2), (y^2 + x^2)\mu - y\mathfrak{y}, \mathfrak{y}\mu - y, y\lambda - x\mu, x\lambda + y\mu - \mathfrak{y}, \mathfrak{y}\lambda - x, \lambda^2 + \mu^2 - 1\}$$

so that $a = xy(x^2 + y^2)$. Yet $\mathcal{V}(xy)$ contains only the orbit of the point $(0, 0)$. We can thus consider $\mathcal{W} = \mathcal{V}(x^2 + y^2)$. The implementation of the Gröbner cover [19, 20] in SINGULAR [6] shows that the singular set of \bar{B} is precisely $\mathcal{W} = \mathcal{V}(x^2 + y^2)$.

Example 3.4 Consider the action of SL_2 on the vector space of 2×2 matrices M_2 :

$$\begin{aligned} \mathrm{SL}_2 \times M_2 &\rightarrow M_2 \\ (\lambda, z) &\mapsto \lambda z \lambda^{-1} \end{aligned}$$

We write

$$\lambda = \begin{bmatrix} \lambda_{11} & \lambda_{12} \\ \lambda_{21} & \lambda_{22} \end{bmatrix}, \quad z = \begin{bmatrix} z_{11} & z_{12} \\ z_{21} & z_{22} \end{bmatrix} \quad \text{and} \quad \mathfrak{z} = \begin{bmatrix} \mathfrak{z}_{11} & \mathfrak{z}_{12} \\ \mathfrak{z}_{21} & \mathfrak{z}_{22} \end{bmatrix}$$

and consider the section defined $P = (\mathfrak{z}_{11}, \mathfrak{z}_{21} - 1)$.

It is a section of degree 1 : The Gröbner basis of the orbit-section ideal is

$$B = (\mathfrak{z}_{11}, \mathfrak{z}_{21} - 1, \mathfrak{z}_{22} - t, \mathfrak{z}_{21} + d) \quad \text{where} \quad t = z_{11} + z_{22}, \quad \text{and} \quad d = z_{22} z_{11} - z_{12} z_{21}.$$

One recognizes the invariants to be the trace and the determinant of the matrix z .

Here

$$\hat{B} = B \cup \{z_{12}\lambda_{21} - z_{11}\lambda_{22} - \lambda_{12}, \lambda_{11} - z_{21}\lambda_{22} + z_{22}\lambda_{21}, \lambda_{12}^2 + t\lambda_{22}\lambda_{12} + d\lambda_{22}^2 + z_{12}, \lambda_{12}\lambda_{21} - z_{21}\lambda_{22}^2 + z_{22}\lambda_{21}\lambda_{22} + 1\}$$

so that $a = z_{12}$. The maximal subset of $\mathcal{V}(z_{12})$ that is invariant is $\mathcal{W} = \mathcal{V}(z_{12}, z_{21}, z_{22} - z_{11})$. It corresponds to the matrices that are scalar multiples of the identity. They are invariants so that their orbits have empty intersection with the section.

Computing the canonical Gröbner cover shows that $\mathcal{V}(z_{12})$ is the singular set of \bar{B} . But the singular set of $B = \bar{B} \cap \mathbb{K}(z)[\mathfrak{z}]$ is the proper invariant subset \mathcal{W} of $\mathcal{V}(z_{12})$. This is obtained by recombining three components of the canonical Gröbner cover.

At this stage it is not clear if one can bypass the computation of the Gröbner cover to determine the singular set. Yet one might wonder if the geometric interpretations of the singular set for specific term order [18, 21, 22] can bring some light on the matter.

3.2 Symmetrizations of a polynomial

In this section we define the symmetrizations of a polynomial. Their definition requires the use of the multiplication map modulo the zero dimensional orbit section ideal. In the next section we shall provide a geometric interpretation for these symmetrizations.

Consider a rational action of \mathcal{G} on $\mathcal{Z} = \overline{\mathbb{K}}^n$ and \mathcal{P} a section of degree e defined by a prime ideal P in $\mathbb{K}[\mathfrak{z}]$. We fix a term order on the variables $\mathfrak{z} = \{\mathfrak{z}_1, \dots, \mathfrak{z}_n\}$ and consider the reduced Gröbner basis B of the orbit-section ideal $I_{\mathcal{P}}$ in $\mathbb{K}(z)[\mathfrak{z}]$.

The coefficients of B belong to and generate $\mathbb{K}(z)^{\mathcal{G}}$ (Theorem 2.4 and 2.6). $\mathbb{K}(z)^{\mathcal{G}}$ is thus the field of definition of the orbit-section ideal $I_{\mathcal{P}}$ and we can consider $I_{\mathcal{P}}^{\mathcal{G}} = I_{\mathcal{P}} \cap \mathbb{K}(z)^{\mathcal{G}}[\mathfrak{z}]$. It is a zero dimensional ideal in $\mathbb{K}(z)^{\mathcal{G}}[\mathfrak{z}]$ and the dimension of $\mathbb{K}(z)^{\mathcal{G}}[\mathfrak{z}]/I_{\mathcal{P}}^{\mathcal{G}}$ as a $\mathbb{K}(z)^{\mathcal{G}}$ -vector space is e .

A polynomial $f \in \mathbb{K}(z)^{\mathcal{G}}[\mathfrak{z}]$ defines an element \bar{f} in the quotient $\mathbb{K}(z)^{\mathcal{G}}[\mathfrak{z}]/I_{\mathcal{P}}^{\mathcal{G}}$. The multiplication map

$$\begin{aligned} m_f : \mathbb{K}(z)^{\mathcal{G}}[\mathfrak{z}]/I_{\mathcal{P}}^{\mathcal{G}} &\rightarrow \mathbb{K}(z)^{\mathcal{G}}[\mathfrak{z}]/I_{\mathcal{P}}^{\mathcal{G}} \\ \bar{g} &\mapsto \bar{f}g \end{aligned}$$

is a linear mapping [4, Proposition 4.1]. Note that $m_{fg} = m_f \circ m_g = m_g \circ m_f$. If f is not a zero divisor modulo $I_{\mathcal{P}}$ then there exists $f_1 \in \mathbb{K}(z)^{\mathcal{G}}[\mathfrak{z}]$ s.t. $f f_1 \equiv 1 \pmod{I_{\mathcal{P}}^{\mathcal{G}}}$. It follows that $\det m_f \neq 0$ and $m_{f_1} = (m_f)^{-1}$. We shall thus define $m_{g/f}$ as $m_{g f_1} = m_g (m_f)^{-1}$ when f is not a zero divisor modulo $I_{\mathcal{P}}^{\mathcal{G}}$.

In the proof of Theorem 2.6 we saw that $I_{\mathcal{P}} \cap \mathbb{K}[\mathfrak{z}] = P$. Hence no element of $\mathbb{K}[\mathfrak{z}] \setminus P$ are zero divisors modulo $I_{\mathcal{P}}^{\mathcal{G}}$. Thus to any element f of the localisation $\mathbb{K}[\mathfrak{z}]_P$ of $\mathbb{K}[\mathfrak{z}]$ at the complement of P corresponds a unique element \bar{f} in $\mathbb{K}(z)^{\mathcal{G}}[\mathfrak{z}]/I_{\mathcal{P}}^{\mathcal{G}}$. The following is thus well defined.

Definition 3.5 For $f \in \mathbb{K}[\mathfrak{z}]_P$ we consider the characteristic polynomial

$$f_{\mathcal{P}}(z, \zeta) = \zeta^e - f_{\mathcal{P}}^{(1)}(z)\zeta^{e-1} + \dots + (-1)^j f_{\mathcal{P}}^{(j)}(z)\zeta^{e-j} + \dots + (-1)^e f_{\mathcal{P}}^{(e)}(z)$$

of the multiplication map m_f by \bar{f} in $\mathbb{K}(z)^{\mathcal{G}}[\mathfrak{z}]/I_{\mathcal{P}}^{\mathcal{G}}$. The coefficients $f_{\mathcal{P}}^{(1)}(z), \dots, f_{\mathcal{P}}^{(e)}(z) \in \mathbb{K}(z)^{\mathcal{G}}$ are the symmetrizations of f w.r.t. the section \mathcal{P} .

Given a reduced Gröbner basis of $I_{\mathcal{P}}$, we can identify a set of monomials that forms a basis of the $\mathbb{K}(z)^{\mathcal{G}}$ -vector space $\mathbb{K}(z)^{\mathcal{G}}[\mathfrak{z}]/I_{\mathcal{P}}^{\mathcal{G}}$ and explicitly write down the matrix of m_f in this basis. The symmetrizations of f defined above can thus be computed algorithmically. At no additional cost, the symmetrizations $f_{\mathcal{P}}^{(1)}(z), \dots, f_{\mathcal{P}}^{(e)}(z) \in \mathbb{K}(z)^{\mathcal{G}}$ are written in terms of the generators $\{r_1, \dots, r_m\}$ of $\mathbb{K}(z)^{\mathcal{G}}$ that are read from the reduced Gröbner basis of $I_{\mathcal{P}}$ according to Theorem 2.6. We formalize these statements.

Proposition 3.6 With the hypotheses and notations of Theorem 2.6, consider the finite set $A \subset \mathbb{N}^n$ such that the set of monomials $\{\mathfrak{z}^{\alpha} \mid \alpha \in A\}$ is the normal set of B . For $f \in \mathbb{K}[\mathfrak{z}]_P$, let $\{\mathfrak{m}_{\alpha, \beta} \mid \alpha, \beta \in A\} \subset \mathbb{K}[\mathfrak{t}]$ be such that $\sum_{\alpha \in A} \mathfrak{m}_{\alpha, \beta} \mathfrak{z}^{\alpha}$ is the normal form of $\mathfrak{z}^{\beta} f$ with respect to \mathfrak{B} . Let $\mathfrak{f}^{(j)} \in \mathbb{K}[\mathfrak{t}]$, $1 \leq j \leq e$, be the coefficients of the characteristic polynomial of the matrix $(\mathfrak{m}_{\alpha, \beta})_{\alpha, \beta \in A}$. The symmetrizations of f are

$$f_{\mathcal{P}}^{(j)}(z_1, \dots, z_n) = \mathfrak{f}^{(j)}(r_1(z), \dots, r_m(z)).$$

The case where \mathcal{P} is a section of degree 1 is particularly favorable. Then $I_{\mathcal{P}} = (\mathfrak{z}_1 - r_1(z), \dots, \mathfrak{z}_n - r_n(z))$ with $r_1, \dots, r_n \in \mathbb{K}(z)^{\mathcal{G}}$, $\mathfrak{B} = \{\mathfrak{z}_1 - \mathfrak{t}_1, \dots, \mathfrak{z}_n - \mathfrak{t}_n\}$ and therefore, for any $f \in \mathbb{K}[\mathfrak{z}]_P$, $\mathfrak{f}^{(1)} = f(\mathfrak{t})$. Hence $f_{\mathcal{P}}^{(1)}(z_1, \dots, z_n) = f(r_1(z), \dots, r_n(z))$.

Example 3.7 SCALINGS IN THE PLANE. We follow up on Example 2.3. We choose $P = (\mathfrak{x}^{\alpha} - \mathfrak{y}^{\beta})$. It defines a section of degree one and the reduced Gröbner basis of $I_{\mathcal{P}}^{\mathcal{G}}$ is $B = \{\mathfrak{x} - r^{\beta}, \mathfrak{y} - r^{\alpha}\}$ where $r = \frac{\mathfrak{y}^{\alpha}}{\mathfrak{x}^{\beta}}$. Thus the symmetrization of f is $f_{\mathcal{P}}^{(1)}(x, y) = f(r^{\beta}, r^{\alpha})$.

Example 3.8 Following up on Example 2.9 where we considered a linear action of SO_2 on $\mathcal{Z} = \overline{\mathbb{K}}^3$ and chose the section defined by $P = (\mathfrak{x})$ so that $I_{\mathcal{P}} = (\mathfrak{x}, \mathfrak{y}^2 - r, \mathfrak{z} - z)$ where $r = x^2 + y^2$.

Consider the polynomials $f_1 = -x(x^2 + y^2 - 1) - yz$ and $f_2 = -y(x^2 + y^2 - 1) + xz$. Neither f_1 nor f_2 are invariant.

A basis for $\mathbb{K}(x, y, z)[\mathfrak{x}, \mathfrak{y}, \mathfrak{z}]/I_{\mathcal{P}}$ is given by the set of monomials $\{1, \mathfrak{y}\}$. In this basis, the multiplication matrices of $f_1(\mathfrak{x}, \mathfrak{y}, \mathfrak{z})$ and $f_2(\mathfrak{x}, \mathfrak{y}, \mathfrak{z})$ are respectively

$$M_1 = \begin{bmatrix} 0 & -zr \\ -z & 0 \end{bmatrix} \quad \text{and} \quad M_2 = \begin{bmatrix} 0 & r(1-r) \\ 1-r & 0 \end{bmatrix}.$$

Hence

$$f_1^{(1)} = -\text{Tr}(M_1) = 0, \quad f_1^{(2)} = \text{Det}(M_1) = -z^2 r,$$

and

$$f_2^{(1)} = -\text{Tr}(M_2) = 0, \quad f_2^{(2)} = \text{Det}(M_2) = r(1-r)^2.$$

Note that $f_{\mathcal{P}}^{(1)}(z)$ is the trace of m_f and the map $f \mapsto f_{\mathcal{P}}^{(1)} \in \mathbb{K}(z)^{\mathcal{G}}$ is a $\mathbb{K}(z)^{\mathcal{G}}$ -linear map. But in general $(\lambda \star f)_{\mathcal{P}}^{(1)} \neq f_{\mathcal{P}}^{(1)}$, contrary to the Reynolds operator.

Example 3.9 In the case of Example 3.7, $(\lambda \star f)_{\mathcal{P}}^{(1)}(x, y) = f(\lambda^{-a} r^{\beta}, \lambda^{-b} r^{\alpha})$ while $f_{\mathcal{P}}^{(1)}(x, y) = f(r^{\beta}, r^{\alpha})$.

3.3 Geometric interpretation and connections

We emphasize in this section the geometric interpretation of the symmetrizations introduced in previous section. This shows that symmetrization generalizes a construction that applies to finite groups.

We have fixed a section \mathcal{P} and a term order on \mathfrak{z} so that B is the reduced Gröbner basis of the orbit section ideal $I_{\mathcal{P}}$ and \mathcal{W} its singular set. For $\bar{z} \in \mathcal{Z} \setminus \mathcal{W}$, $B_{\bar{z}}$ is the Gröbner basis for the ideal of $\mathcal{O}_{\bar{z}} \cap \mathcal{P}$. Thus $(B_{\bar{z}})$ has e zeros $\{\bar{z}^{(1)}, \dots, \bar{z}^{(e)}\}$. They form $\mathcal{O}_{\bar{z}} \cap \mathcal{P}$, possibly with multiplicities.

Proposition 3.10 Consider $f \in \mathbb{K}[\mathfrak{z}]_{\mathcal{P}}$ and $\bar{z} \in \mathcal{Z} \setminus \mathcal{W}$. Let $\{\bar{z}^{(1)}, \dots, \bar{z}^{(e)}\}$ be the e zeros of $B_{\bar{z}}$. For $1 \leq j \leq e$,

$$f_{\mathcal{P}}^{(j)}(\bar{z}) = S_j(f(\bar{z}^{(1)}), \dots, f(\bar{z}^{(e)}))$$

where S_j is the j -th symmetric polynomial in e variables.

PROOF: The eigenvalues of m_f are the evaluations of f at the roots of $(B_{\bar{z}})$, with matching multiplicities [4, Theorem 4.5]. Hence $f_{\mathcal{P}}(z, \zeta) = \prod_{i=1}^e (\zeta - f(\bar{z}^{(i)}))$. \square

Corollary 3.11 If $f \in \mathbb{K}(z)^{\mathcal{G}}$ then $f_{\mathcal{P}}^{(j)} = \binom{j}{e} f^j$.

PROOF: By Proposition 2.5, $\mathbb{K}(z)^{\mathcal{G}} \subset \mathbb{K}[z]_{\mathcal{P}}$ since \mathcal{P} cannot be included in any invariant hypersurface. As an invariant, f is constant on orbits: $f(\bar{z}) = f(\bar{z}^{(1)}) = \dots = f(\bar{z}^{(e)})$. \square

Proposition 3.10 shows that symmetrization as introduced above is a generalization of a construction used in the case of finite groups. Indeed, in the case where \mathcal{G} is a finite group acting regularly and faithfully, we should consider $\mathcal{P} = \mathcal{Z}$ as the section and its degree e is the order of group \mathcal{G} . For $\bar{z} \in \mathcal{Z}$, $\{\bar{z}^{(1)}, \dots, \bar{z}^{(e)}\} = \{\lambda \star \bar{z} \mid \lambda \in \mathcal{G}\}$. Thus

$$f_{\mathcal{P}}(z, \zeta) = \zeta^e - f^{(1)}(z)\zeta^{e-1} + \dots + (-1)^j f^{(j)}(z)\zeta^{e-j} + \dots + (-1)^e f^{(e)}(z) = \prod_{\lambda \in \mathcal{G}} (\zeta - f(\lambda \star z))$$

where $f^{(j)}(z)$ is simply the j -th symmetric function on $\{f(\lambda \star z) \mid \lambda \in \mathcal{G}\}$. The symmetrization $f^{(j)}(z)$, for $1 \leq j \leq e$, are invariant polynomials. As can be read in [28, Proposition 2.6.4], if the variety $\mathcal{V}(F)$ of a finite set of polynomials F is invariant then

$$\mathcal{V}(F) = \mathcal{V}(f^{(i)} \mid f \in F, 1 \leq i \leq e).$$

This proves that any variety invariant under the action of a finite group is the variety of a set of invariant polynomials. The notion of symmetrization w.r.t. a section \mathcal{P} we introduced allows us to provide an analogous result (Theorem 3.12) for the rational action of an algebraic group of positive dimension.

The characteristic polynomial $f_{\mathcal{P}}(z, \zeta)$ of the multiplication map m_f is a polynomial in the elimination ideal $(I_{\mathcal{P}} + (\zeta - f(\mathfrak{z}))) \cap \mathbb{K}(z)[\zeta]$. Up to the distinction between cross-sections and sections, it corresponds to the *invariantization* defined in [12, Section 2.6] for algebraic functions. The purpose of this latter was to provide a constructive approach to the *local* invariantization process that is central in the moving frame construction of differential invariants and invariant derivations in [8]; [12, Theorem 3.9] makes explicit the connection. The meaning of this theorem in the present context is the following : $f_{\mathcal{P}}(z, \zeta)$ is the defining polynomial of a smooth algebraic function that is the unique *local invariant*² that agrees with the values of f on the section \mathcal{P} in the neighborhood of one of its point. Theorem 3.12 below can be seen as a global analogue of a result known to hold locally.

²See [12, Definition 1.3] for the definitions.

3.4 Polynomial systems with symmetry

With the above geometric interpretation of symmetrization we can now prove the main result of the paper : a \mathcal{G} -invariant variety \mathcal{F} is the zero set of a set of invariant functions, outside of a \mathcal{G} -invariant variety \mathcal{W} which is independent of \mathcal{F} . The result is constructive. For a given set of polynomials F , the set \tilde{F} of the symmetrizations of the elements of F is such that $\mathcal{V}(F) \setminus \mathcal{W} = \mathcal{V}(\tilde{F}) \setminus \mathcal{W}$.

The symmetrizations and the singular set \mathcal{W} depends on the choice of a section to the orbits and a term order. Indeed the orbits that do not intersect the section are in \mathcal{W} . On the other hand, the term order decides of the Gröbner basis B of the orbit section ideal $I_{\mathcal{P}}$. The set \mathcal{W} is defined as the maximal set such that for any $\bar{z} \in \mathcal{Z} \setminus \mathcal{W}$ the specialisation $B_{\bar{z}}$ of B at $z \mapsto \bar{z}$ is a Gröbner basis for $\mathcal{O}_{\bar{z}} \cap \mathcal{P}$. In particular \mathcal{W} contains the variety of the denominators of the coefficients of B .

It follows from Proposition 3.10 that

$$\bar{z} \in \mathcal{V}(f_{\mathcal{P}}^{(1)}, \dots, f_{\mathcal{P}}^{(e)}) \setminus \mathcal{W} \Leftrightarrow \mathcal{O}_{\bar{z}} \cap \mathcal{P} \subset \mathcal{V}(f) \setminus \mathcal{W}.$$

The proof of the following result is then similar to the proof in the case of finite groups.

Theorem 3.12 *Consider a section \mathcal{P} of degree e and a term order on $\mathfrak{z} = \{\mathfrak{z}_1, \dots, \mathfrak{z}_n\}$. They determine the reduced Gröbner basis B of $I_{\mathcal{P}}$ in $\mathbb{K}(z)[\mathfrak{z}]$ and its \mathcal{G} -invariant singular set \mathcal{W} .*

Let F be a set of polynomials in $\mathbb{K}[z]$ and assume that its variety \mathcal{F} is \mathcal{G} -invariant. Then

$$\mathcal{V}(f_{\mathcal{P}}^{(i)} \mid f \in F, 1 \leq i \leq e) \setminus \mathcal{W} = \mathcal{F} \setminus \mathcal{W},$$

where $f_{\mathcal{P}}^{(i)}(z) \in \mathbb{K}(z)^{\mathcal{G}}$, $1 \leq i \leq e$, are the symmetrizations of f whose construction is detailed in Proposition 3.6.

Note that the denominators arising in $f_{\mathcal{P}}^{(j)}$ are power products of the denominators of the coefficients of B and thus their varieties lies in \mathcal{W} . Hence $\mathcal{V}(f_{\mathcal{P}}^{(i)} \mid f \in F, 1 \leq i \leq e)$ is to be understood as the variety of the numerators.

PROOF: For $\bar{z} \in \mathcal{Z} \setminus \mathcal{W}$, we note $\{\bar{z}^{(1)}, \dots, \bar{z}^{(e)}\}$ the zeros of $(B_{\bar{z}})$. Each $\bar{z}^{(i)}$ belongs to $\mathcal{O}_{\bar{z}} \cap \mathcal{P}$. As \mathcal{F} is \mathcal{G} -invariant we have $\bar{z} \in \mathcal{F} \setminus \mathcal{W} \Leftrightarrow \{\bar{z}^{(1)}, \dots, \bar{z}^{(e)}\} \subset \mathcal{F} \setminus \mathcal{W}$.

Since

$$\prod_{j=1}^e (\zeta - f(\bar{z}^{(j)})) = \zeta^e - f_{\mathcal{P}}^{(1)}(\bar{z})\zeta^{e-1} + \dots + (-1)^j f_{\mathcal{P}}^{(j)}(\bar{z})\zeta^{e-j} + \dots + (-1)^e f_{\mathcal{P}}^{(e)}(\bar{z})$$

we have $(f(\bar{z}^{(1)}) = 0, \dots, f(\bar{z}^{(e)}) = 0) \Leftrightarrow (f^{(j)}(\bar{z}) = 0, \forall 1 \leq j \leq e)$. \square

Several examples of polynomial systems whose varieties are invariant under a scaling were treated in [13]. These include system of polynomials that are multi-homogeneous according to a set of weights. Indeed [13, Theorem 5.3] can be seen as a special case of the above result.

Example 3.13 *Following on Examples 2.9, 3.3 and 3.8, one observes that $\mathcal{V}(f_1, f_2)$ is invariant under the action of SO_2 since $(f_1, f_2)^t$ is an equivariant map. We determined that outside $\mathcal{W} = \mathcal{V}(x^2 + y^2)$ the reduced Gröbner basis of $I_{\mathcal{P}}$ specialises to the reduced Gröbner basis of the intersection of the orbit of that point with the section \mathcal{P} . Applying the above construction we obtain*

$$\mathcal{V}(f_1, f_2) \setminus \mathcal{W} = \mathcal{V}(f_1^{(1)}, f_1^{(2)}, f_2^{(1)}, f_2^{(2)}) \setminus \mathcal{W} = \mathcal{V}(z^2, (x^2 + y^2 - 1)^2).$$

Example 3.14 *Following up on Example 3.4. Consider the set F consisting of the three polynomials*

$$\begin{aligned} &16 z_{21} z_{12} + 8 z_{11}^2 + 8 z_{22}^2 - 9, \quad 8 z_{11} z_{12} z_{21} - 8 + 24 z_{22} z_{12} z_{21} - 8 z_{22}^2 z_{11} + 8 z_{22}^3 + 9 z_{11}, \\ &128 z_{21}^2 z_{12}^2 - 81 + 512 z_{22}^2 z_{21} z_{12} - 256 z_{22}^3 z_{11} + 128 z_{22}^4 + 72 z_{21} z_{12} + 216 z_{11} z_{22} + 144 z_{22}^2 + 64 z_{11} - 192 z_{22}. \end{aligned}$$

The polynomials are not invariant, except for the first one. Yet, by construction, we know that the variety of F is invariant - F is actually a Gröbner basis for the ideal $(8\operatorname{tr}(z^2) - 9, \operatorname{tr}(z^3) - 1)$. By Proposition 3.12 the variety of F is equal to the variety of

$$\tilde{F} = \{8t^2 - 16d - 9, 8t^3 - 8 - 24td, 128d^2 - 81 - 512t^2d + 128t^4 - 72d + 144t^2 - 192t\}$$

outside of $\mathcal{W} = \mathcal{V}(z_{11} - z_{22}, z_{12}, z_{21})$, the set of matrices that are a scalar multiple of the identity, which are invariant. \tilde{F} is simply obtained from F with the substitution dictated by B , that is

$$z_{11} \rightarrow 0, \quad z_{21} \rightarrow 1, \quad z_{22} \rightarrow t, \quad z_{21} \rightarrow -d.$$

In this particular example $\mathcal{V}(F) \cap \mathcal{W} = \emptyset$ and $\mathcal{V}(\tilde{F}) \cap \mathcal{V}(t^2 - 4d) = \emptyset$, where $\mathcal{V}(t^2 - 4d) \supset \mathcal{W}$. We hence have $\mathcal{V}(\tilde{F}) = \mathcal{V}(F)$. A Gröbner basis for (\tilde{F}) considered as an ideal in $\mathbb{K}[t, d]$, is given by: $(\tilde{F}) = (16 - 27t + 8t^3, 16d + 9 - 8t^2)$.

Example 3.15 The above example generalizes to SL_n acting on the the vector space of $n \times n$ matrices M_n . The invariants $r_1 = -\operatorname{tr}(z), \dots, r_n = (-1)^n \det(z)$ are the coefficients of the characteristic polynomial of $z = (z_{ij})_{1 \leq i, j \leq n}$. Any polynomial system whose variety is invariant is equivalent to a system of polynomials in r_1, \dots, r_n that is obtained by applying the following substitution:

$$[z_{ij}]_{1 \leq i, j \leq n} \rightarrow \begin{bmatrix} 0 & 0 & \dots & 0 & -r_n \\ 1 & 0 & \dots & 0 & -r_{n-1} \\ \vdots & \ddots & & & \vdots \\ \vdots & & \ddots & & \vdots \\ 0 & \dots & & 1 & -r_1 \end{bmatrix}.$$

The right hand side corresponds to the Frobenius normal form of $(z_{ij})_{1 \leq i, j \leq n}$ when the minimal and the characteristic polynomials of z are equal.

As illustrated in the previous example, the symmetrization we introduced is particularly practical when we have a section of degree 1. In this case, the equivalent invariant system is obtained by a simple substitution. The set \tilde{F} has thus the same number of elements as F and is of similar degree when considered as a system in the generating invariants.

Let us conclude by noting that Theorem 3.12 could be extended to invariant semi-algebraic sets $\mathcal{K} = \{z \in \mathbb{R}^n \mid f_1(z) \geq 0, \dots, f_m(z) \geq 0\}$ if we could ensure that the orbits in $\mathcal{K} \cap \mathcal{W}$ intersect the section \mathcal{P} in e points (counting multiplicities), *i.e.* the intersection points are not complex. This is the case in the two examples above, or any time we have a section of degree 1 defined over \mathbb{R} . The argument of [3, Proposition 3.15] that addresses finite groups would indeed generalize to the present context thanks to the analogy drawn in Section 3.3 between the finite group case and the case of an algebraic group of positive dimension.

References

- [1] T. Becker and V. Weispfenning. *Gröbner Bases - A Computational Approach to Commutative Algebra*. Springer-Verlag, New York, 1993.
- [2] L. Bröcker. On symmetric semialgebraic sets and orbit spaces. In *Singularities Symposium—Łojasiewicz 70 (Kraków, 1996; Warsaw, 1996)*, volume 44 of *Banach Center Publ.*, pages 37–50. Polish Acad. Sci., Warsaw, 1998.
- [3] J. Cimprič, S. Kuhlmann, and C. Scheiderer. Sums of squares and moment problems in equivariant situations. *Trans. Amer. Math. Soc.*, 361(2):735–765, 2009.

- [4] D. Cox, J. Little, and D. O’Shea. *Using algebraic geometry*, volume 185 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 2005.
- [5] D. Cox, J. Little, and D. O’Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, Cham, fourth edition, 2015. An introduction to computational algebraic geometry and commutative algebra.
- [6] W. Decker, G.-M. Greuel, G. Pfister, and H. Schönemann. SINGULAR 4-1-1 — A computer algebra system for polynomial computations. <http://www.singular.uni-kl.de>, 2018.
- [7] H. Derksen and G. Kemper. *Computational invariant theory*. Springer-Verlag, 2 edition, 2015. Encyclopaedia of Math. Sc., 130.
- [8] M. Fels and P. J. Olver. Moving coframes. II. Regularization and theoretical foundations. *Acta Applicandae Mathematicae*, 55(2):127–208, 1999.
- [9] K. Gatermann. Semi-invariants, equivariants and algorithms. *Appl. Algebra Engrg. Comm. Comput.*, 7(2):105–124, 1996.
- [10] K. Gatermann. *Computer algebra methods for equivariant dynamical systems*, volume 1728 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 2000.
- [11] E. Hubert and I. Kogan. Rational invariants of a group action. Construction and rewriting. *Journal of Symbolic Computation*, 42(1-2):203–217, 2007.
- [12] E. Hubert and I. Kogan. Smooth and algebraic invariants of a group action. Local and global constructions. *Foundations of Computational Mathematics*, 7(4):355–393, 2007.
- [13] E. Hubert and G. Labahn. Rational invariants of scalings from Hermite normal forms. In *ISSAC 2012*, pages 219–226. ACM Press, 2012.
- [14] E. Hubert and G. Labahn. Scaling invariants and symmetry reduction of dynamical systems. *Foundations of Computational Mathematics*, 13(4):479–516, 2013.
- [15] I. Isaacs. *Algebra: a graduate course*, volume 100 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2009.
- [16] M. Jarić, L. Michel, and R. Sharp. Zeros of covariant vector fields for the point groups: invariant formulation. *J. Physique*, 45(1):1–27, 1984.
- [17] D. Kapur, Y. Sun, and D. Wang. An efficient method for computing comprehensive Gröbner bases. *Journal Symbolic Computation*, 52:124–142, 2013.
- [18] D. Lazard and F. Rouillier. Solving parametric polynomial systems. *Journal of Symbolic Computation*, 42(6):636–667, 2007.
- [19] A. Montes and M. Wibmer. Gröbner bases for polynomial systems with parameters. *J. Symbolic Comput.*, 45(12):1391–1425, 2010.
- [20] A. Montes and M. Wibmer. Software for discussing parametric polynomial systems: the Gröbner cover. In *Mathematical software—ICMS 2014*, volume 8592 of *Lecture Notes in Comput. Sci.*, pages 406–413. Springer, Heidelberg, 2014.
- [21] G. Moroz. Complexity of the resolution of parametric systems of polynomial equations and inequations. In *ISSAC 2006*, pages 246–253. ACM, New York, 2006.
- [22] G. Moroz. Properness defects of projection and minimal discriminant variety. *J. Symbolic Comput.*, 46(10):1139–1157, 2011.

- [23] J. Müller-Quade and T. Beth. Calculating generators for invariant fields of linear algebraic groups. In *Applied algebra, algebraic algorithms and error-correcting codes (Honolulu, HI, 1999)*, volume 1719 of *Lecture Notes in Computer Science*. Springer, 1999.
- [24] A. Parshin and I. Shafarevich, editors. *Algebraic Geometry IV*, volume 55 of *Encyclopaedia of Mathematical Sciences*. Springer-Verlag, Berlin, 1994.
- [25] V. Popov. Sections in invariant theory. In *The Sophus Lie Memorial Conference (Oslo, 1992)*, pages 315–361. Scand. Univ. Press, Oslo, 1994.
- [26] V. Popov and E. Vinberg. Invariant theory. In *Algebraic geometry. IV*, pages 122–278. Springer, 1994.
- [27] M. Rosenlicht. Some basic theorems on algebraic groups. *American Journal of Mathematics*, 78:401–443, 1956.
- [28] B. Sturmfels. *Algorithms in invariant theory*. Texts and Monographs in Symbolic Computation. Springer-Verlag, Vienna, 1993.
- [29] M. Wibmer. Gröbner bases for families of affine or projective schemes. *Journal of Symbolic Computation*, 42(8):803 – 834, 2007.
- [30] P. Worfolk. Zeros of equivariant vector fields: algorithms for an invariant approach. *J. Symbolic Comput.*, 17(6):487–511, 1994.