Rational Invariants of a Group Action

Evelyne Hubert

Rational Invariants of a Group Action

$\mathcal{E}$velyne Hubert*

INRIA MÉDITERRANÉE, FRANCE

Abstract

This article is based on an introductory lecture delivered at the *Journée Nationales de Calcul Formel* that took place at the *Centre International de Recherche en Mathématiques* (2013) in Marseille. We introduce basic notions on algebraic group actions and their invariants. Based on geometric consideration, we present algebraic constructions for a generating set of rational invariants. `http://hal.inria.fr/hal-00839283`

Introduction

Group actions and their invariants is a vast topic on which the greatest algebraists and geometers have contributed. Introducing the topic in its globality and greatness is out of my reach. What I present in those notes are algorithms for problems I encountered in a different context and that were not treated in the active area of computational invariant theory [Stu93, DK02].

I describe a construction of rational invariants of an action of an algebraic group. The class of rational actions to which it applies has not received much attention from the algebraic point of view. Those are nonetheless the actions classically encountered in differential geometry - as for instance conformal or projective actions. My original motivation was to provide an algebraic foundation to the *moving frame* construction as reformulated in [FO99]. This was achieved in a series of articles [HK07a, HK07b, Hub09], an overview of which can be found in [Hub12]. These notes is based on the main results from [HK07a]. Some arguments have been simplified and some of the concepts have been reajusted. The computation of rational invariants is addressed with Gröbner bases, as the most widespread tool for algebraic elimination that that provides canonical representations of an ideal. The algebraic construction makes use of the notion of a *section to the orbits*. This brings a computational advantage, but also makes connections with the concepts of normal forms.

Generating sets of rational invariants serve the purpose of *separating* generic orbits, *i.e.* to characterize objects which are the same under the action of an element in the group. For the generating sets we compute, we furthermore have an algorithm to rewrite any invariants in terms of those. They thus provide a natural set of variables to express a system admitting the group as *symmetry*.

*`http://www-sop.inria.fr/members/Evelyne.Hubert`

1 Group Actions

The action of a group $(\mathcal{G}, \cdot)$ on a set $\mathcal{Z}$ is a map

$$\begin{array}{rccc} \star: & \mathcal{G} \times \mathcal{Z} & \to & \mathcal{Z} \\ & (\lambda, z) & \mapsto & \lambda \star z \end{array}$$

that satisfies the following axioms:

- $1 \star z = z,\ \forall z \in \mathcal{Z}$, where 1 is the identity of the group;
- $\lambda \star (\mu \star z) = (\lambda \cdot \mu) \star z,\ \forall z \in \mathcal{Z},\ \forall \mu, \lambda \in \mathcal{G}$.

We shall consider the action of an affine algebraic group on an affine space $\mathbb{K}^n$. $\mathbb{K}$ is a field of characteristic zero. Mostly $\mathbb{K}$ stands for $\mathbb{C}$. But visualisation are made over the reals $\mathbb{R}$ and computations are performed over $\mathbb{Q}$.

The groups we consider are affine algebraic groups. They are given by an affine algebraic variety $\mathcal{G}$ endowed with a group operation $\cdot : \mathcal{G} \times \mathcal{G} \to \mathcal{G}$ and an inverse $\mathcal{G} \to \mathcal{G}$ given by polynomial maps. To be explicit, we assume that $\mathcal{G}$ is embedded in $\mathbb{K}^s$ and $G \subset \mathbb{K}[\lambda_1, \ldots, \lambda_s]$ is its defining ideal; G is a radical ideal whose irreducible components all have the same dimension, say r. The coordinate ring $\mathbb{K}[\mathcal{G}]$ can be identified with the quotient algebra $\mathbb{K}[\lambda_1, \ldots, \lambda_l]/G$.

Example 1.1 $\mathrm{SL}_n(\mathbb{K})$, *the group of matrices with determinant one, or* $\mathrm{O}_n(\mathbb{K})$ *the group of orthogonal matrices, naturally appear as linear algebraic groups*[1]. *The defining properties for the matrices translate into polynomial equations in the* n^2 *entries of the matrices.*
$\mathrm{O}_n(\mathbb{K})$ *has two components:* $\mathrm{SO}_n = \mathrm{SL}_n \cap \mathrm{O}_n$ *that contains the identity and the set of orthogonal matrices with determinant* -1.

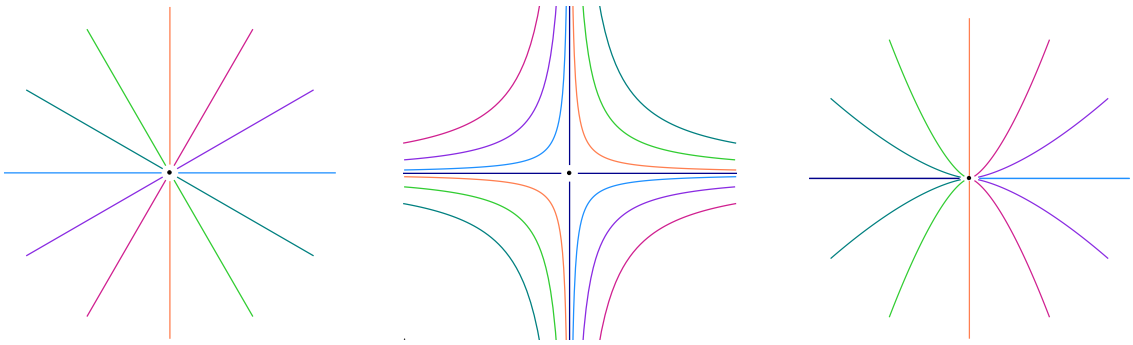
Example 1.2 *The multiplicative group* $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ *can be described by* $\mathbb{K}[\lambda, \mu]/(\lambda\mu - 1)$. *Then* $(\lambda, \mu)^{-1} = (\mu, \lambda)$. *We often spare introducing a second variable and simply write* λ^{-1}. *The coordinate ring is then the ring of Laurent polynomials* $\mathbb{K}[\lambda, \lambda^{-1}]$.

Likewise, the group of invertible matrices $\mathrm{GL}_n(\mathbb{K})$ *is an algebraic group. It is described by* $\mathbb{K}[a_{ij}, h]/(h \det(a_{ij}) - 1)$. *It is abbreviated into* $\mathbb{K}\left[a_{ij}, \det(a_{ij})^{-1}\right]$.

If $\mathcal{Z}$ is a $\mathbb{K}$-linear space and $\rho : \mathcal{G} \to \mathrm{GL}(\mathcal{Z})$ is a group morphism the action given by $\lambda \star z = \rho(\lambda)(z)$ is linear. Those are *representations* and this is a topic on its own. Reference books for the computation of their polynomial invariants include [Stu93, DK02] but there is wealth of results in the more classical texts.

We are interested in the case where $\mathcal{Z}$ is an irreducible affine algebraic variety and $\star$ is a rational action. It is defined by a homomorphism ρ from $\mathcal{G}$ to the birational maps of $\mathcal{Z}$. In practice $\star$ is given by the quotients of polynomials that define a map from some open (dense) subset of $\mathcal{G} \times \mathcal{Z}$ to $\mathcal{Z}$.

[1] Any *affine algebraic group* can actually be realised as a subgroup of matrices. Hence the common use of the name *linear algebraic groups*.



Example 1.4 : orbits of scalings in the plane.

In this presentation, to avoid the difficulty inherent to rational maps, which are not actual maps, we shall settle for *regular actions*. They are given by a morphism $\rho : \mathcal{G} \to \mathrm{Aut}(\mathcal{Z})$ so that $\star : \mathcal{G} \times \mathcal{Z} \to \mathcal{Z}$ is described by a polynomial map.

Definition 1.3 *The orbit of $z \in \mathcal{Z}$ is the set $\mathcal{O}_z = \{\lambda \star z \mid \lambda \in \mathcal{G}\}$.*

The orbit of z is the image of the polynomial map $\mathcal{G} \to \mathcal{Z}$, $\lambda \mapsto \lambda \star z$. An orbit is open in its closure (in Zariski's topology). If it is not closed, its boundary is an invariant subvariety of smaller dimension. There is an invariant open set of $\mathcal{Z}$ where the orbits are of the same (maximal) dimension $d \leq r$.

We present some examples of linear actions in the plane to illustrate the above properties of their orbits. We then give examples of relevant actions which are not linear.

Example 1.4 Scalings. *If we consider the representation $\rho : \lambda \mapsto \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ of $\mathbb{K}^*$ the generic orbits are of dimension 1. Their closures include the origin, which is the only zero dimensional orbit.*

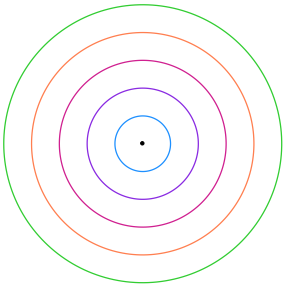
If we consider the representation $\rho : \lambda \mapsto \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$ of $\mathbb{K}^*$, the generic orbits are one-dimensional and closed. There are two one-dimensional orbits whose closure contain the origin, which is the only zero dimensional orbit.

For later reference we consider the representation $\rho : \lambda \mapsto \begin{pmatrix} \lambda^2 & 0 \\ 0 & \lambda^3 \end{pmatrix}$. The situation is similar to the first scaling introduced. But note that the origin is now a singular point of the orbit closure.

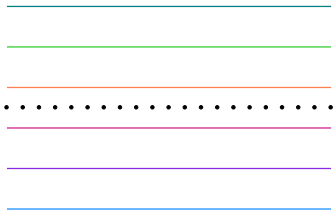
Example 1.5 rotation. *Consider the special orthogonal group $\mathrm{SO}_2(\mathbb{K})$ given by $G = (\lambda_1^2 + \lambda_2^2 - 1) \subset \mathbb{K}[\lambda_1, \lambda_2]$ with representation*

$$\rho : (\lambda_1, \lambda_2) \mapsto \begin{pmatrix} \lambda_1 & -\lambda_2 \\ \lambda_2 & \lambda_1 \end{pmatrix}$$

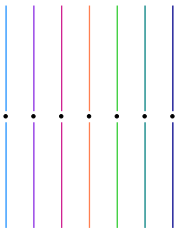
The generic orbits are one dimensional and closed. The origin is the only zero dimensional orbit.



Example 1.5



Example 1.6



Example 1.7

Example 1.6 *Consider the representation*

$$\rho : \lambda \mapsto \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$$

of $(\mathbb{K}, +)$. *The generic orbits are one dimensional and closed. They are the lines parallel to, different from, the horizontal coordinate axis. All the points on the horizontal coordinate axis are zero dimensional orbits.*

Example 1.7 *Consider the representation*

$$\rho : \lambda \mapsto \begin{pmatrix} 1 & 0 \\ 0 & \lambda \end{pmatrix}$$

of $(\mathbb{K}^*, \cdot)$. *The horizontal coordinate axis consists of zero dimensional orbits. The generic orbits are one dimensional and their closures include a point on the horizontal coordinate axis.*

Example 1.8 *The* $\mathbb{K}^* \times \mathbb{K}$ *action given by* $(\lambda, a) \star z = \lambda\, z + a$ *is a simple example of a regular action that is not linear.*

Example 1.9 *The Euclidean group* $\mathrm{O}_n(\mathbb{R}) \ltimes \mathbb{R}^n$ *is the group of isometries of the affine space* $\mathbb{R}^n$.

Example 1.10 Möbius transform. *This is a (non linear) action of* $\mathrm{SL}_2(\mathbb{R})$ *on the plane* $\star : \mathrm{SL}_2(\mathbb{R}) \times \mathbb{R}^2 \to \mathbb{R}^2$.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \star (x, y) = \left(\frac{ac(x^2 + y^2) + (ad + cb)x + bd}{(cx + d)^2 + (cy)^2}, \frac{y}{(cx + d)^2 + (cy)^2} \right)$$

2 Rational invariants

Definition 2.1 *A rational function* $f \in \mathbb{K}(\mathcal{Z})$ *is a* rational invariant *if* $f(\lambda \star z) = f(z)$ *for all* $\lambda \in \mathcal{G}$. *The set of rational invariants forms a field denoted* $\mathbb{K}(\mathcal{Z})^{\mathcal{G}}$.

If $\mathcal{Z}$ is the affine space $\mathbb{K}^n$ then $\mathbb{K}[\mathcal{Z}]$ is the polynomial ring $\mathbb{K}[Z_1, \ldots, Z_n]$. We shall describe the computation of rational invariants in this situation[2].

The orbit $\mathcal{O}_z$ of a point $z \in \mathcal{Z}$ is the image of a polynomial map. The ideal of its (Zariski) closure can be obtained by algebraic elimination. Assume that the action is given by the polynomials $f_1, \ldots, f_n \in \mathbb{K}[\lambda_1, \ldots, \lambda_s, z_1, \ldots, z_n]$ i.e. $\lambda \star z = (f_1(\lambda, z), \ldots, f_n(\lambda, z))$. We shall write

$$(Z - \lambda \star z) \text{ to mean } (Z_1 - f_1(\lambda, z), \ldots, Z_n - f_n(\lambda, z)).$$

The ideal thus formed belongs to $\mathbb{K}(z)[\lambda, Z]$. Consider the elimination ideal

$$O = (G + (Z - \lambda \star z)) \cap \mathbb{K}(z)[Z].$$

For generic z, it provides the ideal of the closure of $\mathcal{O}_z$ by specialization. It is therefore an ideal of dimension d, the dimension of the generic orbits. Because $\mathcal{O}_z = \mathcal{O}_{\mu \star z}$, for all $\mu \in \mathcal{G}$, O has some invariant property. A canonical representation of this ideal must be defined over $\mathbb{K}(z)^G$.

THEOREM 2.2 *The reduced Gröbner basis of $O = (G + (Z - \lambda \star z)) \cap \mathbb{K}(z)[Z]$, with respect to any term order on Z, consists of polynomials in $\mathbb{K}(z)^G[Z]$.*

PROOF: For a given term order, the reduced Gröbner basis of an ideal is unique. Let Q be a reduced Gröbner basis for O for a given term order on Z. As such it consists of monic polynomials in $\mathbb{K}(z)[Z]$.

There is a closed proper subset $\mathcal{W}$ of $\mathcal{Z}$ s.t. for $z \in \mathcal{Z} \setminus \mathcal{W}$ the image of Q under specialization is a (reduced) Gröbner basis for the ideal whose variety is the closure of $\mathcal{O}_z$. Since $\mathcal{O}_z = \mathcal{O}_{\mu \star z}$,

the specializations of Q to z and to $\mu \star z$ bring the same reduced Gröbner basis, for a generic $\mu \in \mathcal{G}$. Therefore $Q \subset \mathbb{K}(z)^G[Z]$. □

The ideal O is actually an unmixed dimensional radical ideal. One can also use the Chow form as canonical representative of O to produce rational invariants [Ros56]. The exhibited set of invariants is then *separating*. As such they form a generating set [Ros56, PV94]. The generation property of the rational invariants of the reduced Gröbner basis has an additional property: they are endowed with an algorithm to rewrite any rational invariant in terms of them.

THEOREM 2.3 *Consider $\{r_1, \ldots, r_k\} \in \mathbb{K}(z)^G$ the coefficients of a reduced Gröbner basis Q of O. Then $\mathbb{K}(z)^G = \mathbb{K}(r_1, \ldots, r_k)$ and we can rewrite any rational invariant $\frac{p}{q}$, with $p, q \in \mathbb{K}[z]$, in terms of those as follows.*

Take a new set of indeterminates $y_1, \ldots, y_k$ and consider the set $Q_y \subset \mathbb{K}[y, Z]$ obtained from Q by substituting r_i by y_i.

Let $a(y, Z) = \sum_{\alpha \in \mathbb{N}^n} a_\alpha(y) Z^\alpha$ and $b(y, Z) = \sum_{\alpha \in \mathbb{N}^n} b_\alpha(y) Z^\alpha$ in $\mathbb{K}[y, Z]$ be the normal forms[3] of $p(Z)$ and $q(Z)$ w.r.t. Q_y.

There exists $\alpha \in \mathbb{N}^n$ s.t. $b_\alpha(g) \neq 0$ and for any such α we have $\frac{p(z)}{q(z)} = \frac{a_\alpha(g)}{b_\alpha(g)}$.

[2]The results generalize to the case where $\mathcal{Z}$ is an irreducible variety instead of an affine space. We only need to consider the ring of polynomial fonctions $\mathbb{K}[\mathcal{Z}]$ or the field of rational functions $\mathbb{K}(\mathcal{Z})$ instead of the polynomial ring $\mathbb{K}[Z]$ or the field of rational functions $\mathbb{K}(z)$. Instead of working in $\mathbb{K}(z)[Z]$ we then work in $\mathbb{K}(\mathcal{Z}) \otimes \mathbb{K}[\mathcal{Z}]$.

[3]For the reductions in $\mathbb{K}[y, Z]$ the term order on Z is extended to a block order $y \ll Z$ so that the set of leading term of Q_y is equal to the set of leading terms of Q.

PROOF: The Gröbner basis Q is reduced and therefore monic so that the set of leading monomials of Q and of Q_y are equal. If $a(y, Z)$ is the reduction of $p(Z)$ w.r.t. Q_y then $a(g, Z)$, obtained by substituting back y_i by r_i, is the normal form of $p(Z)$ w.r.t. Q. Similarly for $b(y, Z)$ and $q(Z)$.

As $O \cap \mathbb{K}[Z] = (0)$, neither $p(Z)$ nor $q(Z)$ belong to O and therefore both $a(g, Z)$ and $b(g, Z)$ are different from 0.

If $\frac{p}{q}$ is a rational invariant then $\frac{p(z)}{q(z)} = \frac{p(Z)}{q(Z)}$ for all $Z \in \mathcal{O}_z$. Thus $p(z)q(Z) - q(z)p(Z) \in O$. Therefore the normal forms $q(z)\, a(r, Z)$ and $p(z)\, b(r, Z)$ of $p(z)q(Z)$ and $q(z)p(Z)$ must be equal. In particular $a(r, Z)$ and $b(r, Z)$ have the same support and this latter is non empty since $a, b \neq 0$. For each α in this common support, we have $q(z)a_\alpha(r) = p(z)b_\alpha(r)$ and therefore $\frac{p(z)}{q(z)} = \frac{a_\alpha(r)}{b_\alpha(r)}$. □

This is the formulation taken in [HK07a]. The result appears to some extent in [MQB99] and is dwelved on in [Kem07].

EXAMPLE 2.4 SCALING. *Consider the first group action of Example 1.4.*

By elimination on the ideal $(1 - \lambda_1\lambda_2, Z_1 - \lambda_1 z_1, Z_2 - \lambda_1 z_2)$ *we obtain* $O = (z_1 Z_2 - z_2 Z_1)$. *The reduced Gröbner basis of* O *for a term order where* $Z_1 < Z_2$ *is* $Q = \{Z_2 - \frac{z_2}{z_1} Z_1\}$. *By Theorem 2.3,* $\mathbb{K}(z_1, z_2)^G = \mathbb{K}(\frac{z_2}{z_1})$.

Let $p = z_1^2 + 4z_1z_2 + z_2^2$ *and* $q = z_1^2 - 3z_2^2$. *We can check that* $\frac{p}{q}$ *is a rational invariant and we set up to write* $\frac{p}{q}$ *as a rational function of* $r = \frac{z_2}{z_1}$. *To this purpose consider* $P = Z_1^2 + 4Z_1Z_2 + Z_2^2$ *and* $Q = Z_1^2 - 3Z_2^2$ *and compute their normal forms* a *and* b *w.r.t.* $\{Z_2 - y\, Z_1\}$. *We have* $a = (1 + 4y + y^2)Z_1^2$ *and* $b = (1 - 3y^2)Z_1^2$. *Thus*

$$\frac{z_1^2 + 4z_1z_2 + z_2^2}{z_1^2 - 3z_2^2} = \frac{1 + 4r + r^2}{1 - 3r^2} \text{ where } r = \frac{z_2}{z_1}.$$

EXAMPLE 2.5 ROTATION. *Consider the group action of Example 1.5. The orbits consist of the origin and the circles with the origin as center. By elimination on the ideal* $(\lambda_1^2 + \lambda_2^2 - 1, Z_1 - \lambda_1 z_1 + \lambda_2 z_2, Z_2 - \lambda_2 z_1 - \lambda_1 z_2)$ *we obtain* $O = \big(Z_1^2 + Z_2^2 - (z_1^2 + z_2^2)\big)$. *By Theorem 2.3,* $\mathbb{K}(z_1, z_2)^G = \mathbb{K}(z_1^2 + z_2^2)$.

Polynomial invariants

We thus proved (constructively) that the field of rational invariants is always finitely generated. This is no surprise since any subfield of $\mathbb{K}(z)$ is finitely generated. The situation is different for the ring of polynomial invariants $\mathbb{K}[z]^{\mathcal{G}}$. Note furthermore that the fraction field of $\mathbb{K}[z]^G$ is included in $\mathbb{K}(z)^G$ but does not need to be equal.

EXAMPLE 2.6 *The two actions in the plane of Example 1.4 given by the representations* $\lambda \mapsto \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$ *and* $\rho : \lambda \mapsto \begin{pmatrix} \lambda^2 & 0 \\ 0 & \lambda^3 \end{pmatrix}$ *of* $\mathbb{K}^*$ *admit no non constant polynomial invariants. Hence* $\mathbb{K}[z]^G = \mathbb{K}$. *Yet the fields of rational invariants are respectively* $\mathbb{K}(\frac{x}{y})$ *and* $\mathbb{K}(\frac{x^3}{y^2})$.

The most general result is that $\mathbb{K}[z]^{\mathcal{G}}$ is finitely generated when $\mathcal{G}$ is a linearly reductive group. These are the groups for which there exists a unique Reynolds operator, a projection from $\mathbb{K}[z]$ to $\mathbb{K}[z]^G$

[DK02, Section 2]. [Der99, DK02] presents an algorithm to compute a set of generators of the algebra of polynomial invariants for the linear action of a reductive group. As for the first proof of finiteness by Hilbert (1890), there is a prominent role there for the ideal $(G+(Z-\lambda\star z))\cap\mathbb{K}[z,Z]+(Z_1,\ldots,Z_n)$ of the Nullcone. A set of generators for $\mathbb{K}[z]^G$ is obtained by applying the Reynolds operator on a set of generators of this ideal.

3 Section to the orbits

DEFINITION 3.1 *An irreducible variety $\mathcal{P}$ is a* section of degree *e of the action $\star$ if there exists a proper algebraic subvariety $\mathcal{W}$ of $\mathcal{Z}$ such that the orbits of $\mathcal{Z}\setminus\mathcal{W}$ intersect $\mathcal{P}$ at exactly e points. Rational section are section of degree* 1.

Assume $P\subset\mathbb{K}[Z]$ is the ideal of the variety $\mathcal{P}$. Then $\mathcal{P}$ is a section of degree e if the ideal

$$I=(G+(Z-\lambda\star z)+P)\cap\mathbb{K}(z)[Z]$$

is zero dimensional and e is the dimension of $\mathbb{K}(z)[Z]/I$ as a $\mathbb{K}(z)$-vector space.

Given an irreducible variety we can then determine if it is a section and compute its degree by computing I. The notion is actually not restrictive. Most irreducible variety of complementary dimension to the orbits are sections to the orbits. Assume the generic orbits have dimension d in $\mathbb{K}^n$. The maximal number of points of intersection of an affine space of codimension d with a generic orbit is defined as the degree of the orbit. Generic affine space of codimension d do intersect generic orbits in that many points.

Though not particularly demanding, the notion of section is computationally useful for groups of positive dimension. Indeed, the ideal I has the same invariant properties as the ideal O and computing a Gröbner basis for I can be easier as this is a zero dimensional ideal. Furthermore, with an appropriate choice of section, the resulting Gröbner basis involves fewer terms and the number of coefficients to consider as generators can be dramatically smaller.

THEOREM 3.2 *The reduced Gröbner basis of I, with respect to any term ordering on Z, consists of polynomials in $\mathbb{K}(z)^G[Z]$.*

The argument is exactly the same as with the ideal O in Theorem 2.2. Just as in Theorem 2.3 we can prove the generating property of the rational invariants appearing as coefficients.

THEOREM 3.3 *Consider $\{r_1,\ldots,r_\kappa\}\in\mathbb{K}(z)^G$ the coefficients of a reduced Gröbner basis Q of I. Then $\mathbb{K}(z)^G=\mathbb{K}(r_1,\ldots,r_\kappa)$ 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 $y_1,\ldots,y_\kappa$ and consider the set $Q_y\subset\mathbb{K}[y,Z]$ obtained from Q by substituting r_i by y_i. Let $a(y,Z)=\sum_{\alpha\in\mathbb{N}^n}a_\alpha(y)Z^\alpha$ and $b(y,Z)=\sum_{\alpha\in\mathbb{N}^n}a_\alpha(y)Z^\alpha$ in $\mathbb{K}[y,Z]$ be the reductions of $p(Z)$ and $q(Z)$ w.r.t. Q_y. There exists $\alpha\in\mathbb{N}^m$ s.t. $b_\alpha(r)\neq 0$ and for any such α we have $\frac{p(z)}{q(z)}=\frac{a_\alpha(r)}{b_\alpha(r)}$.

PROOF: We can proceed just as in the proof of Theorem 2.3; we only need to argue additionally that $p(Z), q(Z) \notin P$.

We first prove that if $\frac{p}{q}$ is a rational invariant, with p and q relatively prime, then p and q are semi-invariants. By hypothesis $p(z)\,q(\lambda \star z) \equiv q(z)\,p(\lambda \star z)$ for all $\lambda \in \mathcal{G}$. Since p and q are relatively prime $p(z)$ divides $p(\lambda \star z)$ that is there exists $a \in \mathbb{K}[z,\lambda]$ s.t. $p(\lambda \star z) \equiv a(\lambda, z)\,p(z) \mod G$. Similarly there exits $b \in h^{-1}\mathbb{K}[z,\lambda]$ s.t. $q(\lambda \star z) \equiv b(\lambda, z)\,q(z) \mod G$. We thus have $p(z)\,q(z)(a(\lambda,z) - b(\lambda,z)) \equiv 0 \mod G$ so that $a \equiv b \mod G$.

As a semi-invariant, if p vanishes at a point z of $\mathcal{Z}$, it vanishes on all the orbit $\mathcal{O}_z$ of z. Assume $p \in P$, that is $p(z) = 0$ for all $z \in \mathcal{P}$. Owing to the definition of the section, any points of $\mathcal{Z}$ outside of a proper algebraic subvariety, is in the orbit of a point on $\mathcal{Z}$. Thus p vanishes on an open dense set of $\mathcal{Z}$. This cannot happen if $p \neq 0$. □

When $\mathcal{P}$ is a rational section the rewriting trivializes into a substitution. Indeed, if the dimension of $\mathbb{K}(z)[Z]/I$ as a $\mathbb{K}(z)$ vector space is 1 then, independently of the chosen term order, the reduced Gröbner basis Q for I is given by $\{Z_i - r_i(z) \,|\, 1 \leq i \leq n\}$ where the $r_i \in \mathbb{K}(z)^G$. In view of Theorem 3.3, $\mathbb{K}(z)^G = \mathbb{K}(r_1, \ldots, r_n)$ and any rational invariant $f(z) \in \mathbb{K}(z)^G$ can be rewritten in terms of r_i by replacing z_i by r_i:

$$f(z_1, \ldots, z_n) = f(\,r_1(z), \ldots, r_n(z)\,), \quad \forall f \in \mathbb{K}(z)^G.$$

EXAMPLE 3.4 SCALING. *We carry on with Example 1.4 and 2.4.*

Choose $P = (Z_1 - 1)$. A reduced Gröbner basis of I is given by $\{Z_1 - 1, Z_2 - \frac{z_2}{z_1}\}$. We can see that Theorem 3.2 is verified and that P defines a rational section. By Theorem 3.3 we know that $r = \frac{z_2}{z_1}$ generates the field of rational invariants $\mathbb{K}(z)^G$. The rewriting algorithm of Theorem 3.3 is a simple replacement. For all $f \in \mathbb{K}(z)^G$ we have $f(z_1, z_2) = f(1, r)$. The simplicity of this rewriting can be constrasted with the one performed in Example 2.4.

EXAMPLE 3.5 ROTATION. *We carry on with Example 1.5 and 2.5.*

Choose $P = (Z_2)$. The reduced Gröbner basis of I w.r.t. any term order is $\{Z_2, Z_1^2 - (z_1^2 + z_2^2)\}$. We can see that Theorem 3.2 is verified and that P defines a cross-section of degree 2. By Theorem 3.3 we know that $r = z_1^2 + z_2^2$ generates the field of rational invariants $\mathbb{K}(z)^G$. In this situation, the rewriting algorithm of Theorem 3.3 consists in substituting z_2 by 0 and z_1^2 by r.

Section, quasi-section, cross-section

The present concept of *section of degree e* appears as *quasi-section* in [PV94]. In [HK07a] we defined *cross-sections of degree e* but the two notions actually differ.

If we consider the scaling $\lambda \star (x, y) = (\lambda^2 x, \lambda^3 y)$ the variety of $P = (Y - X)$ is a section of degree 1. The ideal of the intersection of $\mathcal{P}$ with a generic orbit is

$$I = \left(Y - \frac{x^3}{y^2}, X - \frac{x^3}{y^2}\right).$$

In [HK07a, Definition 3.1] an irreducible ideal P defines a cross-section if the ideal $O + P$ is zero-dimensional and radical. The degree of the cross-section is then the dimension of the $\mathbb{K}$-vector space

$\mathbb{K}(z)[Z]/(O+P)$. This is the number of points of intersection of the closure of a generic orbit with the variety $\mathcal{P}$ of P.

In the above example $O = \left(y^2X^3 - x^3Y^2\right)$ so that the closures of the generic orbits contain the origin. And so does $\mathcal{P}$. There are thus two points of intersections. $\mathcal{P}$ furthermore fails to be a cross-section because O is not a radical ideal. Indeed

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

Both concepts lead to valid computations but the present concept of section is more appropriate.

Example

We examine a linear action of SL_2 on $\mathbb{K}^7$ considered by [Der99]. The linear action of SL_2 on $\mathbb{K}^7$ is given by the following polynomials of $\mathbb{K}[\lambda_1, \ldots, \lambda_4, z_1, \ldots, z_7]$:

$$\begin{gathered}
Z_1 = \lambda_1 z_1 + \lambda_2 z_2, \quad Z_2 = \lambda_3 z_1 + \lambda_4 z_2 \\
Z_3 = \lambda_1 z_3 + \lambda_2 z_4, \quad Z_4 = \lambda_3 z_3 + \lambda_4 z_4 \\
Z_5 = \lambda_1^2 z_5 + 2\lambda_1\lambda_2 z_6 + \lambda_2^2 z_7, \\
Z_6 = \lambda_3\lambda_1 z_5 + \lambda_1\lambda_4 + \lambda_2\lambda_3 z_6 + \lambda_2\lambda_4 z_7, \\
Z_7 = \lambda_3^2 z_5 + 2\lambda_3\lambda_4 z_6 + \lambda_4^2 z_7
\end{gathered}$$

the group being defined by $G = (\lambda_1\lambda_4 - \lambda_2\lambda_3 - 1) \subset \mathbb{K}[\lambda_1, \lambda_2, \lambda_3, \lambda_4]$.

The cross-section defined by $P = (Z_1 + 1, Z_2, Z_3)$ is of degree one. The reduced Gröbner basis (for any term order) of the ideal $I^e \subset \mathbb{K}(z)[Z]$ is given by $\{Z_1+1, Z_2, Z_3, Z_4-r_2, Z_5-r_3, Z_6-r_4, Z_7-r_1\}$ where

$$\begin{gathered}
r_1 = z_7\, {z_1}^2 - 2\, z_2\, z_6\, z_1 + {z_2}^2 z_5, \quad r_2 = z_3\, z_2 - z_1\, z_4, \\
r_3 = \frac{{z_3}^2 z_7 - 2\, z_6\, z_4\, z_3 + z_5\, {z_4}^2}{\left(z_1\, z_4 - z_3\, z_2\right)^2}, \quad r_4 = \frac{z_1\, z_6\, z_4 - z_1\, z_3\, z_7 + z_3\, z_2\, z_6 - z_2\, z_5\, z_4}{z_1\, z_4 - z_3\, z_2}
\end{gathered}$$

By Theorem 3.3, $\mathbb{K}(z)^G = \mathbb{K}(r_1, r_2, r_3, r_4)$. In this case the rewriting of any rational invariant in terms of r_1, r_2, r_3, r_4 consists simply in substituting $(z_1, z_2, z_3, z_4, z_5, z_6, z_7)$ by $(-1, 0, 0, r_2, r_3, r_4, r_1)$. We illustrate this replacement property by rewriting the five generating polynomial invariants computed by [Der99] in terms of r_1, r_2, r_3, r_4:

$$\begin{gathered}
{z_2}^2 z_5 - 2\, z_2\, z_6\, z_1 + z_7\, {z_1}^2 = r_1, \quad z_3\, z_2 - z_1\, z_4 = r_2, \\
{z_3}^2 z_7 - 2\, z_6\, z_4\, z_3 + z_5\, {z_4}^2 = r_3 {r_2}^2, \quad z_1\, z_3\, z_7 - z_3\, z_2\, z_6 + z_2\, z_5\, z_4 - z_1\, z_6\, z_4 = r_4\, r_2, \\
{z_6}^2 - z_7\, z_5 = {r_4}^2 - r_1\, r_3,
\end{gathered}$$

The reduced Gröbner basis of O, relative to the total degree order with ties broken by reverse lexicographical order, has 9 elements:

$$\begin{gathered}
{Z_6}^2 - Z_7\, Z_5 + r_1\, r_3 - {r_4}^2, \quad Z_6\, Z_4 + r_3\, r_2\, Z_2 - r_4\, Z_4 - Z_3\, Z_7, \\
Z_5\, Z_4 - Z_3\, Z_6 + r_3\, r_2\, Z_1 - r_4\, Z_3, \quad Z_3\, Z_2 - Z_1\, Z_4 - r_2, \\
Z_2\, Z_6 - Z_1\, Z_7 + r_4\, Z_2 - \tfrac{r_1}{r_2}\, Z_4, \quad Z_2\, Z_5 + Z_1\, r_4 - Z_6\, Z_1 - \tfrac{r_1}{r_2}\, Z_3, \\
{Z_2}^2 + \tfrac{r_1}{r_3\, {r_2}^2}\, {Z_4}^2 - \tfrac{Z_7}{r_3} - 2\, \tfrac{r_4}{r_3\, r_2}\, Z_4\, Z_2, \quad {Z_1}^2 - \tfrac{Z_5}{r_3} - 2\, \tfrac{r_4}{r_3\, r_2}\, Z_3\, Z_1 + \tfrac{r_1}{r_3\, {r_2}^2}\, {Z_3}^2 \\
Z_2\, Z_1 - \tfrac{r_4}{r_3} - \tfrac{Z_6}{r_3} + \tfrac{r_1}{r_3\, {r_2}^2}\, Z_4\, Z_3 - 2\, \tfrac{r_4}{r_3\, r_2}\, Z_4\, Z_1,
\end{gathered}$$

Though this Gröbner basis is obtained without much difficulty, the example illustrates the advantage obtained by considering the construction with a section: I has much simpler reduced Gröbner basis than O. In particular the number of coefficients to be considered as generators is considerably smaller.

4 Equivalence in geometry and algebra

A group action on $\mathcal{Z}$ defines an equivalence relationship between points on the same orbit. Rational invariants allow to decide of the equivalence of two generic points. Closely connected to the problem of equivalence, the problem of normal forms is in turn intimately linked with the notion of sections. We illustrate this theme on two standard group actions.

A rational invariant f is said to separate the orbits $\mathcal{O}_1$ and $\mathcal{O}_2$ if it is defined at points of both orbits and assumes different values at these points. A set of rational invariants separate the orbits $\mathcal{O}_1$ and $\mathcal{O}_2$ if it contains an invariant that separate these orbits. Finally we say that a finite set R of rational invariants separates generic orbits if there exists a proper subvariety $\mathcal{W}$ in $\mathcal{Z}$ such that R separates the orbits of any two inequivalent points of $\mathcal{Z} \setminus \mathcal{W}$.

In the preceding sections we have emphasized generating sets of rational invariants. The way we have obtained those we can see that they are separating. Conversely, a finite set of separating invariants is generating [Ros56, PV94].

Note that polynomial invariants do not necessarily have any separating property. For instance, we saw in Example 2.6 that an action can have no non trivial polynomial invariants while there are rational invariants. The notion of *separating set of polynomial invariants* [DK02, Section 2.3.2] was introduced relatively recently. The advantage is that there exist finitesuch sets, even for non reductive group. By definition, though, a separating set of polynomial invariants separate what can be separated by polynomial invariants.

Classical invariant theory

$\mathrm{SL}_n(\mathbb{C})$ acts on $\mathbb{C}^n$ linearly. What is known as *classical invariant theory* concerns the induced action of $\mathrm{SL}_n(\mathbb{C})$ on the vector space $\mathbb{C}[x_1, \ldots, x_n]_d$ of homogeneous polynomials of a fixed degree d. The idea is to decide of the equivalence of projective varieties under a linear change of variables.

If $A \in \mathrm{SL}_n(\mathbb{C})$ then $A \star p(x) = p(A\,x)$ defines a (right) action of $\mathrm{SL}_n(\mathbb{C})$ on $\mathbb{C}[x_1, \ldots, x_n]_d$. For instance, for $n = 2$ and $d = 2$,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \star (z_0\,x^2 + z_1\,xy + z_2\,y^2) = (a^2\,z_0 + ac\,z_1 + c^2\,z_2)\,x^2 \\ +(2ab\,z_0 + (bc + ad)\,z_1 + 2cd\,z_2)\,xy + (b^2 z_0 + bd\,z_1 + d^2\,z_2)\,y^2$$

so that the induced representation on the space of conics, whose coordinates are (z_0, z_1, z_2), is

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a^2 & ac & c^2 \\ 2ab & ad + bc & 2cd \\ b^2 & bd & d^2 \end{pmatrix}$$

Applying Theorem 2.3 or Theorem 3.3 we can obtain a generating set of invariants. We have

$$O = \left(Z_1^2 - 4\,Z_2 Z_0 - (z_1^2 - 4\,z_0\,z_2)\right)$$

and choosing the section defined by $P = (Z_1, Z_0 - 1)$ we obtain

$$I = \left(Z_0 - 1, Z_1, Z_2 - \frac{1}{4}(z_1^2 - 4\,z_0 z_1)\right).$$

As we could expect the discriminant is a generating invariant.

The section we chose is of degree 1. The rewriting entailed is then a simple replacement: $z_0 \to 1$, $z_1 \to 0, z_2 \to \frac{1}{4}(z_1^2 - 4\,z_0 z_1)$. It provides a conic that lies at the intersection of the orbit of the given conic and the rational section. It provides a normal form (over $\mathbb{C}$).

Matrix similarity

$\mathrm{GL}_n(\mathbb{K})$ acts on $\mathbb{K}^{n\times n}$ by matrix similarity:

$$\begin{array}{rccc} \star: & \mathrm{GL}_n(\mathbb{K}) \times \mathbb{K}^{n\times n} & \to & \mathbb{K}^{n\times n} \\ & (A,\, M) & \mapsto & AMA^{-1} \end{array}.$$

The reader is invited to check computationally, for small n, that the coefficients of the characteristic polynomial $\chi(t) = t^n - \chi_{n-1}t^{n-1} - \ldots - \chi_0$ of M provide a generating set of rational invariants. Those are polynomials in the entries of $n \times n$ matrices.

To prove the result in general we observe that the companion matrix

$$\begin{pmatrix} . & . & . & \chi_0 \\ 1 & . & . & \chi_1 \\ & \ddots & . & \vdots \\ . & . & 1 & \chi_{n-1} \end{pmatrix}$$

is in the orbit of M if χ is the minimal polynomial of M. The variety of companion matrices provide thus a rational section for the action. The constant entries of the $(n-1)$ first column provide the equations of the rational section. The entries of the last columns are then generating invariants according to Theorem 3.3.

5 Scalings

Scalings form a simple class of actions. They are diagonal actions of the algebraic torus $(\mathbb{K}^*)^r$ They have a prominent role in applications despite their simplicity. Remarkably, the computations pertaining to their invariants can be performed with linear algebra. In [HL12] we show how to compute a mininal generating set, a rational section and the rewrite rules. They are deduced from a unimodular multiplier providing the Hermite form of the integer matrix of powers describing the

scaling. Those results are extended in [HL13] to address the parameter reduction in models of mathematical biology. In this section we give a foretaste for some scalings in the plane.

We consider a scaling of the plane

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

defined by some $a, b \in \mathbb{N}$ that are relatively prime. The ideal of the orbit of $(x, y) \in \mathbb{K}^2 \setminus \{(0, 0)\}$ is then given by

$$O = (x^b Y^a - y^a X^b).$$

Thus $g = \frac{y^a}{x^b}$ is a generating invariant. A generic affine line in $\mathbb{K}^2$ is a section of degree $\max(a, b)$. If we choose defined by $P = (X - 1)$, it defines a section of degree a since the ideal of the intersection of the orbit of $(x, y) \in \mathbb{K}^2 \setminus \{(0, 0)\}$ with the variety $\mathcal{P}$ of P is

$$I = \left(X - 1, Y^a - \frac{y^a}{x^b} \right).$$

A smarter choice of section is provided by the Bezout coefficients $\alpha, \beta \in \mathbb{Z}$ s.t. $\alpha\, a - \beta\, b = 1$. Assume for simplicity that $\alpha, \beta \in \mathbb{N}$. If we choose $P = (X^\alpha - Y^\beta) : (XY)^\infty$ then the ideal of the intersection of the orbit of $(x, y) \in \mathbb{K}^2 \setminus \{(0, 0)\}$ with the variety $\mathcal{P}$ of P is

$$I = \left(X - \left(\frac{y^a}{x^b} \right)^\beta,\ Y - \left(\frac{y^a}{x^b} \right)^\alpha \right).$$

We thus have a rational section.

This generalizes for scalings in all dimensions. Furthermore, for those actions, a minimal set of generators and rewrite rules are obtained with linear algebra operations solely. The key ingredient is the computation of Hermite normal forms. All the necessary information is read on the unimodular multiplier.

In the case above, for instance, all the needed information is read from

$$\underbrace{\begin{bmatrix} a & b \end{bmatrix}}_{\text{scaling}} \underbrace{\begin{bmatrix} \alpha & -b \\ -\beta & a \end{bmatrix}}_{\text{multiplier}} = \underbrace{\begin{bmatrix} 1 & 0 \end{bmatrix}}_{\text{Hermite form}}.$$

The last column of the multiplier provides the powers of a generating invariant. The first column descibes the rational section. Finally, the rewriting $x \to \left(\frac{y^a}{x^b} \right)^\beta$, $y \to \left(\frac{y^a}{x^b} \right)^\alpha$ inferred by the section can be read as the last row of the inverse of the unimodular multiplier, which is

$$\begin{bmatrix} a & b \\ \beta & \alpha \end{bmatrix}.$$

We refer to [HL12, HL13] for the general case.

References

[Der99] H. Derksen. Computation of invariants for reductive groups. *Adv. Math.*, 141(2):366–384, 1999.

[DK02] H. Derksen and G. Kemper. *Computational invariant theory.* Invariant Theory and Algebraic Transformation Groups I. Springer-Verlag, Berlin, 2002. Encyclopaedia of Math. Sc., 130.

[FO99] M. Fels and P. J. Olver. Moving coframes. II. Regularization and theoretical foundations. *Acta Appl. Math.*, 55(2):127–208, 1999.

[HK07a] E. Hubert and I. A. Kogan. Rational invariants of a group action. Construction and rewriting. *Journal of Symbolic Computation*, 42(1-2):203–217, 2007.

[HK07b] E. Hubert and I. A. Kogan. Smooth and algebraic invariants of a group action. Local and global constructions. *Foundations of Computational Mathematics*, 7(4), 2007.

[HL12] E. Hubert and G. Labahn. Rational invariants of scalings from Hermite normal forms. In *Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation*, ISSAC '12, pages 219–226, New York, NY, USA, 2012. ACM.

[HL13] E. Hubert and G. Labahn. Scaling invariants and symmetry reduction of dynamical systems. *Foundations of Computational Mathematics*, 2013.

[Hub09] E. Hubert. Differential invariants of a Lie group action: syzygies on a generating set. *Journal of Symbolic Computation*, 44(3):382–416, 2009.

[Hub12] E. Hubert. Algebraic and differential invariants. In F. Cucker, T. Krick, A. Pinkus, and A. Szanto, editors, *Foundations of computational mathematics, Budapest 2011*, number 403 in London Mathematical Society Lecture Note Series. Cambrige University Press, 2012.

[Kem07] G. Kemper. The computation of invariant fields and a new proof of a theorem by Rosenlicht. *Transformation Groups*, 12:657–670, 2007.

[MQB99] 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*, pages 392–403. Springer, Berlin, 1999.

[PV94] V. L. Popov and E. B. Vinberg. Invariant theory. In A. N. Parshin and I. R. Shafarevich, editors, *Algebraic geometry. IV*, volume 55 of *Encyclopaedia of Mathematical Sciences*, pages 122–278. Springer-Verlag, Berlin, 1994.

[Ros56] M. Rosenlicht. Some basic theorems on algebraic groups. *American Journal of Mathematics*, 78:401–443, 1956.

[Stu93] B. Sturmfels. *Algorithms in invariant theory.* Texts and Monographs in Symbolic Computation. Springer-Verlag, Vienna, 1993.