

Rational Invariants of a Group Action. Construction and Rewriting.

Evelyne Hubert

INRIA Sophia Antipolis, France

Irina A. Kogan

North Carolina State University, USA

Abstract

Geometric constructions applied to a rational action of an algebraic group lead to a new algorithm for computing rational invariants. A finite generating set of invariants appears as the coefficients of a reduced Gröbner basis. The algorithm comes in two variants. In the first construction the ideal of the graph of the action is considered. In the second one the ideal of a cross-section is added to the ideal of the graph. Zero-dimensionality of the resulting ideal brings a computational advantage. In both cases, reduction with respect to the computed Gröbner basis allows to express any rational invariant in terms of the generators.

Key words: rational invariants, algebraic group actions, cross-section, Gröbner basis, differential invariants, moving frame

1991 MSC: 13A50, 13P10, 14L24, 14Q99, 53A55 .

1. Introduction

We present an algebraic construction for a finite set of rational invariants of a rational group action on an affine space. The exhibited finite set is shown to be a set of generators of the field of rational invariants. It is furthermore endowed with a simple algorithm to express any rational invariant in terms of the generators.

The construction is algorithmic and can easily be implemented in general purpose computer algebra systems or software specialized in Gröbner basis computations. This is illustrated by a MAPLE worksheet¹ where the examples of the paper are treated. As

URLs: www.inria.fr/cafe/Evelyne.Hubert (Evelyne Hubert), www.math.ncsu.edu/~iakogan (Irina A. Kogan).

¹ available at www.inria.fr/cafe/Evelyne.Hubert/Publi/RationalInvariants

we shall explain, there is no obstruction in generalizing the results to an action on an irreducible variety instead of an affine space.

The algorithm comes in two variants. For the first construction we consider the graph of the action as did Rosenlicht (1956), Vinberg and Popov (1994)², and Müller-Quade and Beth (1999)³. We point out the connections with these previous works in the text. Our proofs are independent and provide an original approach. We show that the coefficients of a reduced Gröbner basis of the ideal of the graph of the action are invariant. We prove that these coefficients generate the field of rational invariants by exhibiting an algorithm for rewriting any rational invariant in terms of them. In the second construction we consider a section of the graph. That is, from the algebraic point of view, we consider the sum of the ideal of the graph with the ideal of a *cross-section* to the orbits. The *graph-section ideal* thus obtained is of dimension zero and that brings an advantage when it comes to Gröbner basis computation.

As showed in (Hubert and Kogan, 2006), the second construction provides algebraic foundations to the moving frame construction of Fels and Olver (1999). We introduce *replacement invariants*, the algebraic counterpart of Cartan's *normalized invariants*. Those are tuples of algebraic functions of rational invariants. Any invariant can be rewritten in terms of them by just substituting the coordinate functions by the corresponding component from the tuple. The components of a replacement invariants thus form a generating set for *algebraic invariants*, which we define as algebraic functions of rational invariants. The relations among the components are simple: they are given by the equations of the cross-section. The latter can be chosen with a large amount of freedom and this is fruitful in applications. For these reasons we believe that algebraic and replacement invariants deserve more attention.

Diverse fields of application of algebraic invariant theory are presented by Derksen and Kemper (2002, Chapter 5). Some of the applications can be addressed with rational invariants. One of the advantage is that, contrary to the ring of polynomial invariants, the field of rational invariants is always finitely generated. The present construction together with the simple rewriting algorithm can bring computational benefits. Our interest in applications to differential problems motivates our choice to consider rational actions. Even if we start with an affine or even linear action on the zeroth order jet space, the prolongation of the action to the higher order jet spaces is usually rational.

The paper is structured as follows. In Section 2 we introduce the action of an algebraic group on the affine space and the graph of the action. This leads to the first construction of a set of generating rational invariants. The second construction is given after the introduction of the cross-section to the orbits in Section 3. Section 4 provides additional examples.

Acknowledgements

We would like to thank Teresa Krick, Liz Mansfield, Peter Olver, Eric Schost, Michael Singer, and Agnes Szanto, for valuable discussions and suggestions on the paper.

² We are indebted to a referee of the conference MEGA for pointing out this reference that motivated us to push in new directions some of the results presented then. See (Hubert and Kogan, 2006).

³ We would like to thank H. Derksen for suggesting comparison with this reference after we made public our first preprint.

2. Graph of a group action and rational invariants

We give a definition of a rational action of an algebraic group on an affine space. Two additional hypotheses are necessary for our constructions. We recall the definition for the graph of the action. It plays a central role in our constructions. The first variant of the algorithm for computing a generating set of rational invariants, together with an algorithm for expressing any rational invariant in terms of them, is presented in this section.

For exposition convenience we assume that the field \mathbb{K} is algebraically closed. As the construction proposed in this section relies solely on Gröbner basis computations, it can be performed in the field of definition of the data (usually \mathbb{Q} or \mathbb{F}_p).

2.1. Rational action of an algebraic group

We consider an algebraic group that is defined as an algebraic variety \mathcal{G} in the affine space \mathbb{K}^l . The group operation and the inverse are given by polynomial maps. The neutral element is denoted by e . We shall consider an action of \mathcal{G} on an affine space $\mathcal{Z} = \mathbb{K}^n$.

Throughout the paper $\lambda = (\lambda_1, \dots, \lambda_l)$ and $z = (z_1, \dots, z_n)$ denote indeterminates while $\bar{\lambda} = (\bar{\lambda}_1, \dots, \bar{\lambda}_l)$ and $\bar{z} = (\bar{z}_1, \dots, \bar{z}_n)$ denote points in $\mathcal{G} \subset \mathbb{K}^l$ and $\mathcal{Z} = \mathbb{K}^n$ respectively. The coordinate ring of \mathcal{Z} and \mathcal{G} are respectively $\mathbb{K}[z_1, \dots, z_n]$ and $\mathbb{K}[\lambda_1, \dots, \lambda_l]/G$, where G is a radical unmixed dimensional ideal. By $\bar{\lambda} \cdot \bar{\mu}$ we denote the image of $(\bar{\lambda}, \bar{\mu})$ under the group operation while $\bar{\lambda}^{-1}$ denotes the image of $\bar{\lambda}$ under the inversion map.

DEFINITION 2.1 *A rational action of an algebraic group \mathcal{G} on the affine space \mathcal{Z} is a rational map $g: \mathcal{G} \times \mathcal{Z} \rightarrow \mathcal{Z}$ that satisfies the following two properties*

- (1) $g(e, \bar{z}) = \bar{z}, \forall \bar{z} \in \mathcal{Z}$
- (2) $g(\bar{\mu}, g(\bar{\lambda}, z)) = g(\bar{\mu} \cdot \bar{\lambda}, z)$, whenever both $(\bar{\lambda}, \bar{z})$ and $(\bar{\mu} \cdot \bar{\lambda}, \bar{z})$ are in the domain of definition of g .

A rational action is uniquely determined by a n -tuple of rational functions of $\mathbb{K}(\lambda, z)$ whose domain of definition is a dense open set of $\mathcal{G} \times \mathcal{Z}$. We can bring these rational functions to their least common denominator $h \in \mathbb{K}[\lambda, z]$ without affecting the domain of definition. In the rest of the paper the action is thus given by

$$g(\bar{\lambda}, \bar{z}) = (g_1(\bar{\lambda}, \bar{z}), \dots, g_n(\bar{\lambda}, \bar{z})) \text{ for } g_1, \dots, g_n \in h^{-1}\mathbb{K}[\lambda_1, \dots, \lambda_l, z_1, \dots, z_n] \quad (1)$$

ASUMPTION 2.2 *We make the additional assumptions*

- (1) for all $\bar{z} \in \mathcal{Z}$, $h(\lambda, \bar{z}) \in \mathbb{K}[\lambda]$ is not a zero-divisor modulo G . This says that the domain of definition of $g_{\bar{z}}: \bar{\lambda} \mapsto g(\bar{\lambda}, \bar{z})$ contains a non-empty open set of each component of \mathcal{G} .
- (2) for all $\bar{\lambda} \in \mathcal{Z}$, $h(\bar{\lambda}, z) \in \mathbb{K}[z]$ is different from zero. In other words, for every element $\bar{\lambda} \in \mathcal{G}$ there exists $\bar{z} \in \mathcal{Z}$, such that $(\bar{\lambda}, \bar{z})$ is in the domain of definition g .

The following three examples serve as illustration throughout the text.

EXAMPLE 2.3 SCALING. *Consider the multiplicative group given by $G = (1 - \lambda_1 \lambda_2) \subset \mathbb{K}[\lambda_1, \lambda_2]$. The neutral element is $(1, 1)$ and $(\bar{\mu}_1, \bar{\mu}_2) \cdot (\bar{\lambda}_1, \bar{\lambda}_2)^{-1} = (\bar{\mu}_1 \bar{\lambda}_2, \bar{\mu}_2 \bar{\lambda}_1)$. We consider the scaling action of this group on \mathbb{K}^2 . It is given by the following polynomials of $\mathbb{K}[\lambda_1, \lambda_2, z_1, z_2]$: $g_1 = \lambda_1 z_1, \quad g_2 = \lambda_1 z_2$.*

EXAMPLE 2.4 TRANSLATION+REFLECTION. Consider the group that is the direct product of the additive group and the group of two elements $\{1, -1\}$, its defining ideal in $\mathbb{K}[\lambda_1, \lambda_2]$ being $G = (\lambda_2^2 - 1)$. The neutral element is $(0, 1)$ while $(\bar{\mu}_1, \bar{\mu}_2) \cdot (\bar{\lambda}_1, \bar{\lambda}_2)^{-1} = (\bar{\mu}_1 - \bar{\lambda}_1, \bar{\mu}_2 \bar{\lambda}_2)$. We consider its action on \mathbb{K}^2 as translation parallel to the first coordinate axis and reflection w.r.t. this axis. It is defined by the following polynomials of $\mathbb{K}[\lambda_1, \lambda_2, z_1, z_2]$: $g_1 = z_1 + \lambda_1$, $g_2 = \lambda_2 z_2$.

EXAMPLE 2.5 ROTATION. Consider the special orthogonal group given by $G = (\lambda_1^2 + \lambda_2^2 - 1) \subset \mathbb{K}[\lambda_1, \lambda_2]$ with $e = (1, 0)$ and $(\bar{\mu}_1, \bar{\mu}_2) \cdot (\bar{\lambda}_1, \bar{\lambda}_2)^{-1} = (\bar{\mu}_1 \bar{\lambda}_1 + \bar{\mu}_2 \bar{\lambda}_2, \bar{\mu}_2 \bar{\lambda}_1 - \bar{\mu}_1 \bar{\lambda}_2)$. Its linear action on \mathbb{K}^2 is given by the following polynomials of $\mathbb{K}[\lambda_1, \lambda_2, z_1, z_2]$:

$$g_1 = \lambda_1 z_1 - \lambda_2 z_2, \quad g_2 = \lambda_2 z_1 + \lambda_1 z_2.$$

An element of the group acts as a rotation around the origin.

2.2. Graph of the action and orbits

The graph of the action is the image $\mathcal{O} \subset \mathcal{Z} \times \mathcal{Z}$ of the map $(\bar{\lambda}, \bar{z}) \mapsto (\bar{z}, g(\bar{\lambda}, \bar{z}))$ that is defined on a dense open set of $\mathcal{G} \times \mathcal{Z}$. We have $\mathcal{O} = \{(\bar{z}, \bar{z}') \mid \exists \bar{\lambda} \in \mathcal{G} \text{ s.t. } \bar{z}' = g(\bar{\lambda}, \bar{z})\} \subset \mathcal{Z} \times \mathcal{Z}$.

We introduce a new set of variables $Z = (Z_1, \dots, Z_n)$ and the ideal

$$J = G + (Z - g(\lambda, z)) \subset h^{-1}\mathbb{K}[\lambda, z, Z]$$

where $(Z - g(\lambda, z))$ stands for $(Z_1 - g_1(\lambda, z), \dots, Z_n - g_n(\lambda, z))$. The set \mathcal{O} is dense in its closure $\bar{\mathcal{O}}$, and $\bar{\mathcal{O}}$ is the algebraic variety of the ideal:

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

Since G is radical and unmixed dimensional so is J because of the linearity in Z . If $G = \bigcap_{i=0}^{\kappa} G^{(i)}$ is the prime decomposition of G then we have the following prime decomposition of J :

$$(G + (Z - g(\lambda, z))) = \bigcap_{i=0}^{\kappa} (G^{(i)} + (Z - g(\lambda, z))).$$

The prime ideal $O^{(i)} = (G^{(i)} + (Z - g(\lambda, z))) \cap \mathbb{K}[z, Z]$ is therefore a component of O . The ideals $O^{(i)}$, however, need not be all distinct.

The set \mathcal{O} is symmetric: if $(\bar{z}, \bar{z}') \in \mathcal{O}$ then $(\bar{z}', \bar{z}) \in \mathcal{O}$. By the Nullstellensatz the ideal O is also symmetric: $p(Z, z) \in O$ if $p(z, Z) \in O$. Since $J \cap \mathbb{K}[z] = (0)$, $O \cap \mathbb{K}[z] = (0)$ and therefore $O \cap \mathbb{K}[Z] = (0)$ also.

Given the action (1), a set of generators for $O \subset \mathbb{K}[z, Z]$ is obtained by elimination. More explicitly we can compute a Gröbner basis (Becker and Weispfenning, 1993) of O .

PROPOSITION 2.6 Let g' be the n -tuple of numerators of g : $g' = hg = (hg_1, \dots, hg_n) \in (\mathbb{K}[\lambda, z])^n$. Consider a term order s.t. $z \cup Z \ll \lambda \cup \{y\}$ where y is a new indeterminate. If Q is a Gröbner basis for $G + (hZ - g') + (yh - 1)$ according to this term order then $Q \cap \mathbb{K}[z, Z]$ is a Gröbner basis of O according the induced term order on $z \cup Z$.

PROOF: Take $J' = (G + (Z - g)) \cap \mathbb{K}[\lambda, z, Z]$ and note that $J' = (G + (hZ - g')) : h^\infty$ where g' is the numerator of g . Given a basis Λ of G and g explicitly, a Gröbner basis of J is obtained thanks to (Becker and Weispfenning, 1993, Proposition 6.37, Algorithm 6.6). We recognize that O is an elimination ideal of J' , namely $O = J' \cap \mathbb{K}[z, Z]$. A Gröbner basis for O is thus obtained by (Becker and Weispfenning, 1993, Proposition 6.15, Algorithm 6.1). \square

We mainly use the extension O^e of O in $\mathbb{K}(z)[Z]$. If Q is a Gröbner basis of O w.r.t. a term order $z \ll Z$ then Q is also a Gröbner basis for O^e w.r.t. the term order induced on Z (Becker and Weispfenning, 1993, Lemma 8.93). It is nonetheless often preferable to compute a Gröbner basis of O^e over $\mathbb{K}(z)$ directly.

The *orbit* of $\bar{z} \in \mathcal{Z}$ is the image $\mathcal{O}_{\bar{z}}$ of the rational map $g_{\bar{z}}: \mathcal{G} \mapsto \mathcal{Z}$ defined by $g_{\bar{z}}(\bar{\lambda}) = g(\bar{\lambda}, \bar{z})$. We then have the following specialization property (see for instance Cox et al., 1992, Exercise 7).

PROPOSITION 2.7 *Let Q be a Gröbner basis for O^e for a given term order on 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 of Q under the specialization $z \mapsto \bar{z}$ is a Gröbner basis for the ideal whose variety is the closure of the orbit of \bar{z} .*

Therefore, for $\bar{z} \in \mathcal{Z} \setminus \mathcal{W}$, the dimension of the orbit of \bar{z} is equal to the dimension of $O^e \subset \mathbb{K}(z)[Z]$ (Cox et al., 1992, Section 9.3, Theorem 8). In the rest of the paper this dimension is denoted by s .

EXAMPLE 2.8 SCALING. *Consider the group action of Example 2.3. The set of orbits consists of 1-dimensional punctured straight lines through the origin and a single zero-dimensional orbit, the origin. By elimination on the ideal $J = (1 - \lambda_1 \lambda_2, Z_1 - \lambda_1 z_1, Z_2 - \lambda_1 z_2)$ we obtain $O = (z_1 Z_2 - z_2 Z_1)$. Take \mathcal{W} to consist solely of the origin. For $\bar{z} \in \mathcal{Z} \setminus \mathcal{W}$ the closure of the orbit of \bar{z} is the algebraic variety of $(\bar{z}_1 Z_2 - \bar{z}_2 Z_1)$*

EXAMPLE 2.9 TRANSLATION+REFLECTION. *Consider the group action of Example 2.4. By elimination on the ideal $J = (\lambda_2^2 - 1, Z_1 - z_1 - \lambda_1, Z_2 - \lambda_2 z_2)$ we obtain $O = (Z_2^2 - z_2^2)$. The orbit of a point $\bar{z} = (\bar{z}_1, \bar{z}_2)$ with $\bar{z}_2 \neq 0$ consists of two lines parallel to the first coordinate axis, while the latter is the orbit of all points with $\bar{z}_2 = 0$*

EXAMPLE 2.10 ROTATION. *Consider the group action of Example 2.5. The orbits consist of the origin and the circles with the origin as center. By elimination on the ideal $J = (\lambda_1^2 + \lambda_2^2 - 1, Z_1 - \lambda_1 z_1 + \lambda_2 z_2, Z_2 - \lambda_2 z_1 - \lambda_1 z_2)$ we obtain $O = (Z_1^2 + Z_2^2 - z_1^2 - z_2^2)$.*

2.3. Rational invariants

We construct a finite set of generators for the field of rational invariants. Our construction brings out a simple algorithm to rewrite any rational invariant in terms of them. The required operations are restricted to computing a Gröbner basis and normal forms. Those are implemented in most computer algebra systems. We provide a comparison with related results by Rosenlicht (1956); Vinberg and Popov (1994); Müller-Quade and Beth (1999).

DEFINITION 2.11 A rational function $r \in \mathbb{K}(z)$ is a rational invariant if $r(g(\lambda, z)) = r(z) \pmod{G}$.

The set of rational invariants forms a field⁴ $\mathbb{K}(z)^G$. We show in the following lemma that rational invariants are the quotients of *semi-invariants*. Although this result is to be expected, we have not found it in the literature for the case of rational actions.

LEMMA 2.12 If p/q is a rational invariant, with $p, q \in \mathbb{K}[z]$ relatively prime, then there exists $\alpha \in h^{-1}\mathbb{K}[\lambda, z]$ s.t.

$$p(g(\lambda, z)) \equiv \alpha(\lambda, z)p(z) \pmod{G} \text{ and } q(g(\lambda, z)) \equiv \alpha(\lambda, z)q(z) \pmod{G}$$

PROOF: By hypothesis $p(z)q(g(\lambda, z)) \equiv q(z)p(g(\lambda, z)) \pmod{G}$. Since p and q are relatively prime $p(z)$ divides $p(g(\lambda, z))$ modulo G , that is there exists $\alpha \in h^{-1}\mathbb{K}[z, \lambda]$ s.t. $p(g(\lambda, z)) \equiv \alpha(\lambda, z)p(z) \pmod{G}$. Similarly there exists $\beta \in h^{-1}\mathbb{K}[z, \lambda]$ s.t. $q(g(\lambda, z)) \equiv \beta(\lambda, z)q(z) \pmod{G}$. We thus have $p(z)q(z)(\alpha(\lambda, z) - \beta(\lambda, z)) \equiv 0 \pmod{G}$ so that $\alpha \equiv \beta \pmod{G}$. \square

We show that the coefficients of the Gröbner basis for O^e are invariant and generate $\mathbb{K}(z)^G$.

LEMMA 2.13 If $q(z, Z)$ belongs to O then $q(g(\bar{\lambda}, z), Z)$ belongs to O^e for all $\bar{\lambda} \in \mathcal{G}$.

PROOF: A point $(\bar{z}, \bar{z}') \in \mathcal{Z} \times \mathcal{Z}$ belongs to \mathcal{O} if there exists $\bar{\mu} \in \mathcal{G}$ s.t. $\bar{z}' = g(\bar{\mu}, \bar{z})$. Then for a generic $\bar{\lambda} \in \mathcal{G}$, $\bar{z}' = g(\bar{\mu} \cdot \bar{\lambda}^{-1}, g(\bar{\lambda}, \bar{z}))$. Therefore $(g(\bar{\lambda}, \bar{z}), \bar{z}') \in \mathcal{O}$. Thus if $q(z, Z) \in O$ then $q(g(\bar{\lambda}, \bar{z}), \bar{z}') = 0$ for all $(\bar{z}, \bar{z}') \in \mathcal{O}$. By Hilbert Nullstellensatz the numerator of $q(g(\bar{\lambda}, z), Z)$ belongs to O and therefore $q(g(\bar{\lambda}, z), Z) \in O^e$. \square

Following Becker and Weispfenning (1993, Definition 5.29), a set of polynomials is reduced, for a given term order, if the leading coefficients of the elements are equal to 1 and each element is in normal form with respect to the others. Given a term order on Z a polynomial ideal in $\mathbb{K}(z)[Z]$ has a unique reduced Gröbner basis (Becker and Weispfenning, 1993, Theorem 5.3).

THEOREM 2.14 The reduced Gröbner basis of O^e with respect to any term order on Z consists of polynomials in $\mathbb{K}(z)^G[Z]$.

PROOF: Let $Q = \{q_1, \dots, q_\kappa\}$ be the reduced Gröbner basis of O^e for a given term order on Z . By Lemma 2.13 $q_i(g(\bar{\lambda}, z), Z)$ belongs to O^e . It has the same support⁵ as q_i . As $q_i(g(\bar{\lambda}, z), Z)$ and $q_i(z, Z)$ have the same leading monomial, $q_i(g(\bar{\lambda}, z), Z) - q_i(z, Z)$ is in normal form with respect to Q . As this difference belongs to O^e , it must be 0. The coefficients of q_i are therefore invariant. \square

Rosenlicht (1956, paragraph before Theorem 2) points out that the coefficients of the Chow form of O^e over $\mathbb{K}(z)$ form a set of separating rational invariants. As proved by Rosenlicht (1956, Theorem 2); Vinberg and Popov (1994, Lemma 2.1), such a set is generating for $\mathbb{K}(z)^G$.

⁴ Though we do not use this fact but rather retrieve it otherwise, it is worth noting that, as a subfield of $\mathbb{K}(z)$, the field of rational invariants is always finitely generated (van der Waerden, 1971).

⁵ The support here is the set of terms in Z with non zero coefficients.

Vinberg and Popov (1994, Lemma 2.4) showed the existence of a subset of $\mathbb{K}(z)^G[Z]$ that generates O^e . Theorem 2.14 offers a constructive version of this result, which could actually have been deduced directly from it since a Gröbner basis of an ideal has its coefficients in the field of definition of any set of generators of this ideal. They showed furthermore that the set of the coefficients of such a family of generators *separates generic orbits* (Vinberg and Popov, 1994, Theorem 2.3) and therefore generates $\mathbb{K}(z)^G$ (Rosenlicht, 1956, Theorem 2), (Vinberg and Popov, 1994, Lemma 2.1). From those results we deduce that the set of coefficients of a reduced Gröbner basis of O^e generates $\mathbb{K}(z)^G$. The next theorem provides an alternative proof of this result, providing additionally a rewriting algorithm. To prove generation we indeed exhibit an algorithm that allows to rewrite any rational invariant in terms of the coefficients of a reduced Gröbner basis.

In the case of linear actions Müller-Quade and Beth (1999) showed that O^e is equal to the ideal obtained by extending the coefficients of the ideal $J_{\mathbb{K}(z)/\mathbb{K}(z)^G} = ((Z - z) \cap \mathbb{K}(z)^G[Z])$ to $\mathbb{K}(z)$. The three page proof relies on the result of Rosenlicht about the separation property of rational invariants for generic orbits Rosenlicht (1956). Using results about the characterization of subfields of $\mathbb{K}(z)$ obtained by Müller-Quade and Steinwandt (1999), they deduce that the coefficients of the Gröbner basis of O^e generate the field of rational invariants. We claim the result for rational actions and our approach is more direct. The generating properties of the coefficients of the reduced Gröbner basis of O^e follow directly from the rewriting algorithm that we prove below. The rewriting algorithm presented in this paper can be compared to Algorithm 1.10 of Müller-Quade and Steinwandt (1999). Some core operations are the same but the specifications are different: Algorithm 1.10 of Müller-Quade and Steinwandt (1999) is a membership test to a subfield of $\mathbb{K}(z)$ given by a set of generators. A reinterpretation is needed to turn it into a rewriting algorithm.

LEMMA 2.15 *Let $\frac{p}{q}$ be a rational invariant, $p, q \in \mathbb{K}[z]$. Then $p(Z)q(z) - q(Z)p(z) \in O$.*

PROOF: Since $\frac{p}{q}$ is an invariant $\frac{p(\bar{z})}{q(\bar{z})} = \frac{p(g(\bar{\lambda}, \bar{z}))}{q(g(\bar{\lambda}, \bar{z}))}$ for all $(\bar{\lambda}, \bar{z})$ where this expression is defined. Thus $a(\bar{z}', \bar{z}) = p(\bar{z}')q(\bar{z}) - q(\bar{z}')p(\bar{z}) = 0$ for all $(\bar{z}, \bar{z}') \in \mathcal{O} = \{(\bar{z}, \bar{z}') \mid \exists \bar{\lambda} \in \mathcal{G} \text{ s.t. } \bar{z}' = g(\bar{\lambda}, \bar{z})\} \subset \mathcal{Z} \times \mathcal{Z}$. In other words the polynomial $a(Z, z) = p(Z)q(z) - q(Z)p(z) \in \mathbb{K}[Z, z]$ is zero at each point of \mathcal{O} . Since the algebraic variety of O is the closure $\bar{\mathcal{O}}$ of \mathcal{O} and that \mathcal{O} is dense in $\bar{\mathcal{O}}$ we can conclude that $a(Z, z) \in O$ by Hilbert Nullstellensatz. \square

Assume a polynomial ring over a field is endowed with a given term order. A polynomial p is in *normal form* w.r.t. a set Q of polynomials if p involves no term that is a multiple of a leading term of an element in Q . A *reduction* w.r.t. Q is an algorithm that, given p , returns a polynomial p' in normal form w.r.t. Q s.t. $p = p' + \sum_{q \in Q} a_q q$ and no leading term of any $a_q q$ is larger than the leading term of p . Such an algorithm is detailed by Becker and Weispfenning (1993, Algorithm 5.1). It consists in rewriting the terms that are multiple of the leading terms of the elements of Q by polynomials involving only terms that are lower. Note that if the leading coefficients of Q are 1 then no division occurs. When Q is a Gröbner basis w.r.t. the given term order, the reduction of a polynomial p is unique in the sense that p' is then the only polynomial in normal form w.r.t. Q in the equivalence class $p + (Q)$.

THEOREM 2.16 Consider $\{r_1, \dots, r_\kappa\} \in \mathbb{K}(z)^G$ the coefficients of a reduced Gröbner basis Q of O^e . Then $\mathbb{K}(z)^G = \mathbb{K}(r_1, \dots, r_\kappa)$ 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, \dots, y_κ 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 reductions⁶ of $p(Z)$ and $q(Z)$ w.r.t. Q_y . There exists $\alpha \in \mathbb{N}^n$ 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: It is sufficient to prove the second part of the statement. The Gröbner basis Q is reduced and therefore monic. The sets 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 $a(r, Z)$, 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 $O^e \cap \mathbb{K}[Z] = (0)$, neither $p(Z)$ nor $q(Z)$ belong to O^e and therefore both $a(r, Z)$ and $b(r, Z)$ are different from 0. By Lemma 2.15 $q(z)p(Z) \equiv p(z)q(Z) \pmod{O^e}$ and thus the normal forms of the two polynomials modulo O^e are equal: $q(z)a(r, Z) = p(z)b(r, Z)$. Thus $a(r, Z)$ 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 $\frac{p(z)}{q(z)} = \frac{a_\alpha(r)}{b_\alpha(r)}$. \square

EXAMPLE 2.17 SCALING. We consider the group action given in Example 2.3. A reduced Gröbner basis of O^e is $Q = \{Z_2 - \frac{z_2}{z_1} Z_1\}$. By Theorem 2.14, $\mathbb{K}(z_1, z_2)^G = \mathbb{K}(\frac{z_2}{z_1})$.

Let $p = z_1^2 + 4z_1z_2 + z_2^2$ and $q = z_1^2 - 3z_2^2$. We can check that p/q is a rational invariant and we set up to write p/q as a rational function of $r = z_2/z_1$. 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. $\{Z_2 - yZ_1\}$ according to a term order where $Z_1 < Z_2$. 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 2.18 TRANSLATION+REFLECTION. We consider the group action given in Example 2.4. A reduced Gröbner basis of O^e is $Q = \{Z_2^2 - z_2^2\}$. By Theorem 2.14, $\mathbb{K}(z_1, z_2)^G = \mathbb{K}(z_2^2)$.

EXAMPLE 2.19 ROTATION. We consider the group action given in Example 2.5. A reduced Gröbner basis of O^e is $Q = \{Z_1^2 + Z_2^2 - (z_1^2 + z_2^2)\}$. By Theorem 2.14, $\mathbb{K}(z_1, z_2)^G = \mathbb{K}(z_1^2 + z_2^2)$.

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 functions $\mathbb{K}[\mathcal{Z}]$ or the field of rational functions $\mathbb{K}(\mathcal{Z})$ instead of the polynomial ring $\mathbb{K}[z]$ or the field of rational function $\mathbb{K}(z)$. Instead of working in $\mathbb{K}(z)[Z]$ we then work in $\mathbb{K}(\mathcal{Z}) \otimes \mathbb{K}[\mathcal{Z}]$.

⁶ 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 .

3. Cross-section and rational invariants

Given a cross-section we construct a generating set of rational invariants endowed with a rewriting algorithm. The method is the same as the one presented in the previous section but applies to only a section of the graph. In previous section we considered an ideal of the dimension of the generic orbits. Here we consider a zero-dimensional ideal. This improves the efficiency of the algorithms that rely on Gröbner bases computation.

We use Noether normalization to prove the existence of a cross-section. The construction thus relies on selecting an element in an open subset of a certain affine space. This is always possible over an infinite field. Though the presentation is done with an algebraically closed field \mathbb{K} , which is therefore infinite, the construction is meant to be realized in characteristic zero (i.e. over \mathbb{Q}), or over a sufficiently large field.

This second construction does not entail a deterministic algorithm for the computation of rational invariants. Yet the freedom of choice is extremely fruitful for practical computations and applications.

3.1. Cross-section

Geometrically speaking a *cross-section of degree d* is a variety that intersects generic orbits in d simple points. We give a definition in terms of ideals for it is closer to the actual computations. We give its geometric content in a proposition afterward. At the same time we define algebraically the cross-section, we define the *graph-section ideal I^e* .

DEFINITION 3.1 *Let P be a prime ideal of $\mathbb{K}[Z]$ of complementary dimension to the generic orbits, i.e. if O^e is of dimension s then P is of codimension s . The ideal P defines a cross-section to the orbits of the rational action $g : \mathcal{G} \times \mathcal{Z} \rightarrow \mathcal{Z}$ if the ideal $I^e = O^e + P$ of $\mathbb{K}(z)[Z]$ is radical and zero dimensional. We say that P defines a cross-section of degree d if d is the dimension of $\mathbb{K}(z)[Z]/I^e$ as a $\mathbb{K}(z)$ -vector space.*

Indeed the algebra $\mathbb{K}(z)[Z]/I^e$ is a finite-dimensional $\mathbb{K}(z)$ -vector space since I^e is zero dimensional (Becker and Weispfenning, 1993, Theorem 6.54). A basis for it is provided by the terms in Z that are not multiple of the leading terms of a Gröbner basis of I^e (Becker and Weispfenning, 1993, Proposition 6.52). Let us note here that an ideal of $\mathbb{K}(z)[Z]$ is zero dimensional iff any Gröbner basis of it has an element whose leading term is $Z_i^{d_i}$, for all $1 \leq i \leq n$ (Becker and Weispfenning, 1993, Theorem 6.54). We can also check algorithmically that $O^e + P$ is zero dimensional by using for instance (Becker and Weispfenning, 1993, Theorem 8.20).

The cross-section is thus the variety \mathcal{P} of P . The geometric properties of this variety are explained by the following proposition. Geometric necessary conditions for a variety to be a cross-section is that it is of complementary dimension and transversal to the orbits at its generic points. This can be restated as conditions on the tangent spaces. As we can compute the tangent space to the orbits from the knowledge of the action, transversality can be easily checked by linear algebra operations, possibly after specializing z to a generic \bar{z} of \mathcal{P} .

PROPOSITION 3.2 *Let P define a cross-section \mathcal{P} of degree d . There is a closed set $\mathcal{S} \subset \mathcal{Z}$ s.t. the closure of the orbit of any $\bar{z} \in \mathcal{Z} \setminus \mathcal{S}$ intersects \mathcal{P} in d simple points.*

PROOF: Let Q be a reduced Gröbner basis for $I^e = O^e + P$. Similarly to Proposition 2.7, the image $Q_{\bar{z}}$ of Q under the specialization $z \mapsto \bar{z}$ is a Gröbner basis for $O_{\bar{z}} + P$ in $\mathbb{K}[Z]$ for all \bar{z} in \mathcal{Z} outside of a closed set \mathcal{W} . Thus $I_{\bar{z}} = O_{\bar{z}} + P$ is zero dimensional and the dimension of $\mathbb{K}[Z]/I_{\bar{z}}$ as a vector space over \mathbb{K} is d .

By the Jacobian criterion for regularity and the prime avoidance theorem (Eisenbud, 1994, Corollary 16.20 and Lemma 3.3) there is a $n \times n$ minor f of the Jacobian matrix of Q that is not included in any prime divisor of I^e . Therefore f is not a zero divisor in $\mathbb{K}(z)[Z]/I^e$ which is a product of fields. There exists thus $f' \in \mathbb{K}(z)[Z]$ s.t. $f f' \equiv 1 \pmod{I^e}$.

Provided that \bar{z} is furthermore chosen so that the denominators of f and f' do not vanish, f specializes into a $n \times n$ minor $f_{\bar{z}}$ of the Jacobian matrix of $Q_{\bar{z}}$ and we have $f_{\bar{z}} f'_{\bar{z}} \equiv 1 \pmod{I_{\bar{z}}}$ for the specialization $f'_{\bar{z}}$ of f' . So $f_{\bar{z}}$ belongs to no prime divisors of $I_{\bar{z}}$ and thus $I_{\bar{z}}$ is radical (Eisenbud, 1994, Corollary 16.20). We take \mathcal{S} to be the union of \mathcal{W} with the algebraic set associated to the product of the denominators of f and f' . That the number of points of intersection is d is shown by (Eisenbud, 1994, Proposition 2.15). \square

This property shows that the cross-sections of degree $d = 1$ and $d > 1$ are respectively the sections and the quasi-sections defined by Vinberg and Popov (1994, Paragraph 2.5). The existence of quasi-section is insured by (Vinberg and Popov, 1994, Proposition 2.7), while a criterion for the existence of a section is described by Vinberg and Popov (1994, Paragraph 2.5 and 2.6). Our terminology elaborates on the one used by Rosenlicht (1956) and Fels and Olver (1999).

By a non-constructive argument Vinberg and Popov (1994, Section 2.5) show that $\mathbb{K}(\mathcal{P})$ is isomorphic to $\mathbb{K}(z)^G$ when \mathcal{P} is a cross-section of degree 1. If \mathcal{P} is a cross-section of degree $d > 1$ then $\mathbb{K}(\mathcal{P})$ is an algebraic extension of $\mathbb{K}(z)^G$ of degree d . We retrieve this result from a constructive angle in Hubert and Kogan (2006).

Our approach is inspired by the geometric construction of Fels and Olver (1999): almost any algebraic variety of complementary dimension provides a cross-section of some degree. The existence of a cross-section is proved by Noether normalization theorem, which provides an alternative definition of the dimension of an ideal (Shafarevich, 1994, Section 6.2).

THEOREM 3.3 *To each point $(a_{ij})_{1 \leq i \leq n, 0 \leq j \leq n}$ of an open set of $\mathbb{K}^{n(n+1)}$ we can associate a linear cross-section to the orbits defined by*

$$P = \left(a_{i0} - \sum_{j=1}^n a_{ij} Z_j \mid 1 \leq i \leq s \right).$$

PROOF: Assume that a Gröbner basis Q of O^e w.r.t. a term order $Z_1, \dots, Z_s \ll Z_{s+1}, \dots, Z_n$ is s.t. there is an element of Q with leading term $Z_i^{d_i}$, for some $d_i \in \mathbb{N} \setminus \{0\}$, for all $s+1 \leq i \leq n$ and there is no element of Q independent of $\{Z_{s+1}, \dots, Z_n\}$. Then Q is a Gröbner basis for the extension of O^e to $\mathbb{K}(z)(Z_1, \dots, Z_s)[Z_{s+1}, \dots, Z_n]$ (Becker and Weispfenning, 1993, Lemma 8.93). For (a_{10}, \dots, a_{s0}) in an open set of \mathbb{K}^s the specialization $Q_a \subset \mathbb{K}[Z_{s+1}, \dots, Z_n]$ of Q under $Z_i \mapsto a_{i0}$ is a Gröbner basis (Cox et al., 1992, Exercise 7). Therefore $Q_a \cup \{Z_1 - a_{10}, \dots, Z_s - a_{s0}\}$ is a Gröbner basis by Buchberger's criteria (Becker and Weispfenning, 1993, Theorem 5.48 and 5.66). It is

a Gröbner basis of a zero dimensional ideal (Becker and Weispfenning, 1993, Theorem 6.54). We can thus take P to be generated by $\{Z_1 - a_{10}, \dots, Z_s - a_{s0}\}$.

We can always retrieve the situation assumed above by a change of variables thanks to Noether normalization theorem (Greuel and Pfister, 2002, Theorem 3.4.1). Inspecting the proof we see that we can choose a change of variables given by a matrix $(a_{ij})_{1 \leq i, j \leq n}$ with the vector of entries a_{ij} in \mathbb{K}^{n^2} outside of some algebraically closed set. The set $\{a_{i0} - \sum_{1 \leq j \leq n} a_{ij} Z_j \mid 1 \leq i \leq s\}$ thus defines a cross-section. \square

The choice of a cross section introduces a non deterministic aspect to the algebraic construction proposed in next section. An analysis of the probability of success in characteristic 0 would be based on the measure of a correct test sequence as studied by Giusti and Heintz (1993, Theorem 3.5 and 3.7.2); Giusti et al. (1993, Section 3.2); Krick et al. (2001, Section 4.1).

PROPOSITION 3.4 *Assume that $P \subset \mathbb{K}[Z]$ defines a cross-section and that $O = \bigcap_{i=0}^{\tau} O^{(i)}$ is the prime decomposition of O . Then*

$$O + P = \bigcap_{i=0}^{\tau} (O^{(i)} + P) \quad \text{and} \quad (O^{(i)} + P) \cap \mathbb{K}[Z] = P.$$

PROOF: We can easily check that $\bigcap_{i=0}^{\tau} (O^{(i)} + P) \subset O + P$ because $O + P$ is radical. The converse inclusion is trivial.

For the second equality, note first that $P \subset (O^{(i)} + P) \cap \mathbb{K}[z, Z]$. The projection of the variety of $O^{(i)} \subset \mathcal{X} \times \mathcal{Z}$ is thus contained in \mathcal{P} . We show that the projection is exactly \mathcal{P} . We can assume that the numbering is such that $O^{(i)} = (G^{(i)} + (z - g(\lambda, Z))) \cap \mathbb{K}[z, Z]$ where $G^{(i)}$ is a minimal prime of G (see Section 2). By Assumption 2.2, for any \bar{z} in \mathcal{Z} , and therefore in \mathcal{P} , there exists $\bar{\lambda}$ in the variety of $G^{(i)}$ s.t. $g(\bar{\lambda}, \bar{z})$ is defined. Above each point of \mathcal{P} there is a point in the variety of $O^{(i)}$. \square

3.2. Rational invariants revisited

The following theorems provide a construction of a generating set of rational invariants together with an algorithm to rewrite any rational invariant in terms of generators. The method is the same as in Section 2.3 but applied to the ideal graph-section ideal I^e rather than to the graph ideal O^e . The computational advantage comes from the fact that I^e is zero dimensional.

If G is a prime ideal we can actually choose a coordinate cross-section. In other words, P can be taken as the ideal generated by a set of the following form: $\{Z_{j_1} - a_1, \dots, Z_{j_s} - a_s\}$ for (a_1, \dots, a_s) in \mathbb{K}^s . In this case we can remove s variables for the computation.

THEOREM 3.5 *The reduced Gröbner basis of I^e with respect to any term ordering on Z consists of polynomials in $\mathbb{K}(z)^G[Z]$.*

PROOF: The union of a reduced Gröbner basis of O^e and P forms a generating set for $I^e = O^e + P$. The coefficients of a basis for P are in \mathbb{K} , while the coefficients of a reduced basis for O^e belong to $\mathbb{K}(z)^G$ due to Theorem 2.14. Since the coefficients of a generating set for I^e belong to $\mathbb{K}(z)^G$, so do the coefficients of the reduced Gröbner basis with respect to any term ordering. \square

LEMMA 3.6 *If p/q is a non zero rational invariant, with $p, q \in \mathbb{K}[z]$ relatively prime, then neither $p(Z)$ nor $q(Z)$ belong to P .*

PROOF: We prove the result for p , the result being then true for q too. By Lemma 2.12 $p(g(\lambda, z)) \equiv \alpha(\lambda, z)p(z) \pmod{G}$. Thus if $p \in P$, or equivalently if p vanishes on \mathcal{P} , it vanishes on an open subset of \mathcal{Z} (Proposition 3.2). So p must be zero. This is not the case and thus $p \notin P$. \square

THEOREM 3.7 *Consider $\{r_1, \dots, r_\kappa\} \in \mathbb{K}(z)^G$ the coefficients of a reduced Gröbner basis Q of I^e . Then $\mathbb{K}(z)^G = \mathbb{K}(r_1, \dots, r_\kappa)$ 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, \dots, y_κ 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 2.16; we only need to argue additionally that $p(Z), q(Z) \notin I^e$. As $I^e \cap \mathbb{K}[Z] = P$ and $p(Z), q(Z) \notin P$, by Lemma 3.6, it follows that $p(Z) \notin I^e$. \square

When P defines a cross-section of degree 1, the rewriting trivializes into a *replacement*. Indeed, if the dimension of $\mathbb{K}(z)[Z]/I^e$ as a $\mathbb{K}(z)$ vector space is 1 then, independently of the chosen term order, the reduced Gröbner basis Q for I^e is given by $\{Z_i - r_i(z) \mid 1 \leq i \leq n\}$ where the $r_i \in \mathbb{K}(z)^G$. In view of Theorem 3.7, $\mathbb{K}(z)^G = \mathbb{K}(r_1, \dots, r_n)$ and any rational invariant $r(z) \in \mathbb{K}(z)^G$ can be rewritten in terms of r_i by replacing z_i by r_i :

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

In the next section we generalize this replacement property to the case of a cross-section of any degree by introducing *replacement invariants* that are n -tuples of algebraic functions of the rational invariants.

EXAMPLE 3.8 SCALING. *We carry on with the action considered in Example 2.3 and 2.17.*

Choose $P = (Z_1 - 1)$. A reduced Gröbner basis of I^e is given by $\{Z_1 - 1, Z_2 - \frac{z_2}{z_1}\}$. We can see that Theorem 3.5 is verified and that P defines a cross-section of degree 1. By Theorem 3.7 we know that $r = z_2/z_1$ generates the field of rational invariants $\mathbb{K}(z)^G$. In this situation, the cross section is of degree 1 and the rewriting algorithm of Theorem 3.7 is a simple replacement. For all $p \in \mathbb{K}(z)^G$ we have $p(z_1, z_2) = p(1, r)$.

EXAMPLE 3.9 TRANSLATION+REFLECTION. *We carry on with the action considered in Example 2.4 and 2.18.*

Choose $P = (Z_1 - Z_2)$ to define the cross-section. A reduced Gröbner basis of I^e is given by $\{Z_1 - Z_2, Z_2^2 - z_2^2\}$. The cross-section is thus of degree 2.

EXAMPLE 3.10 ROTATION. We carry on with the action considered in Example 2.5 and 2.19.

Choose $P = (Z_2)$. The reduced Gröbner basis of I^e w.r.t. any term order is $\{Z_2, Z_1^2 - (z_1^2 + z_2^2)\}$. We can see that Theorem 2.14 is verified and that P defines a cross-section of degree 2. By Theorem 3.7 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 3.7 consists in substituting z_2 by 0 and z_1^2 by r .

3.3. Replacement invariants

We introduce algebraic invariants, that is algebraic elements over $\mathbb{K}(z)^G$. Such invariants are seldom used in algebraic invariant theory. Yet algebraic functions occur everywhere in differential invariant theory (see Example 4.2). We show in (Hubert and Kogan, 2006) that the replacement invariants that we introduce here take the role of Cartan's *normalized invariants*.

Let \mathcal{P} be a cross-section of degree d defined by a prime ideal P of $\mathbb{K}[Z]$. The field of rational functions on \mathcal{P} is denoted by $\mathbb{K}(\mathcal{P})$. It is the fraction field of the integral domain $\mathbb{K}[Z]/P = \mathbb{K}[\mathcal{P}]$. We introduce d replacement invariants associated to \mathcal{P} .

DEFINITION 3.11 An algebraic invariant is an element of the algebraic closure $\overline{\mathbb{K}(z)^G}$ of $\mathbb{K}(z)^G$.

A reduced Gröbner basis Q of $I^e = O^e + P$ is contained in $\mathbb{K}(z)^G[Z]$ (Theorem 3.5) and therefore is a reduced Gröbner basis of $I^G = I^e \cap \mathbb{K}(z)^G[Z]$. The dimension of $\mathbb{K}(z)^G[Z]/I^G$ as a $\mathbb{K}(z)^G$ -vector space is therefore equal to the dimension d of $\mathbb{K}(z)[Z]/I^e$ as a $\mathbb{K}(z)$ -vector space. Consequently the ideal I^G has d zeros $\xi = (\xi_1, \dots, \xi_n)$ with $\xi_i \in \overline{\mathbb{K}(z)^G}$ (Eisenbud, 1994, Proposition 2.15). We call such a tuple (ξ_1, \dots, ξ_n) a $\overline{\mathbb{K}(z)^G}$ -zero of I^G . A $\overline{\mathbb{K}(z)^G}$ -zero of I^G is a $\overline{\mathbb{K}(z)^G}$ -zero of I^e and conversely.

DEFINITION 3.12 A replacement invariant is a $\overline{\mathbb{K}(z)^G}$ -zero of $I^G = I^e \cap \mathbb{K}(z)^G[Z]$, i.e. a n -tuple $\xi = (\xi_1, \dots, \xi_n)$ of algebraic invariants that forms a zero of I^e .

Thus d replacement invariants $\xi^{(1)}, \dots, \xi^{(d)}$ are associated to a cross-section of degree d . The name owes to next theorem which can be compared with Thomas replacement theorem discussed by Fels and Olver (1999, page 38).

THEOREM 3.13 Let $\xi = (\xi_1, \dots, \xi_n)$ be a replacement invariant. If $r \in \mathbb{K}(z)^G$ then $r(z_1, \dots, z_n) = r(\xi_1, \dots, \xi_n)$ in $\overline{\mathbb{K}(z)^G}$.

PROOF: Write $r = \frac{p}{q}$ with p, q relatively prime. By Lemma 2.15, $p(z)q(Z) - q(z)p(Z) \in O^e \subset I^e$ and therefore $p(Z) - \frac{p(z)}{q(z)}q(Z) = p(Z) - r(z)q(Z) \in I^e$. Since ξ is a zero of I^e , we have $p(\xi) - r(z)q(\xi) = 0$. By Lemma 3.6 $p(Z), q(Z)$ can not belong to P and therefore cannot be zero divisors modulo I^e because of Proposition 3.4. Thus $q(\xi) \neq 0$ and the conclusion follows. \square

For any replacement invariant ξ we have $\mathbb{K}(\xi) \cong \mathbb{K}(\mathcal{P})$. The concept of replacement invariant is thus useful for computing implicitly with algebraic invariants. All the rational

invariants can be trivially written in terms of the components of ξ and the ideal of the cross-section, which is chosen quite freely, provides the relations among the components of ξ .

EXAMPLE 3.14 SCALING. Consider the multiplicative group from Example 2.3, 2.8, 2.17, 3.8. We considered the cross-section of degree 1 defined by $P = (Z_1 - 1)$. There is single replacement invariant $\xi = (1, \frac{z_2}{z_1})$, which can be read off the reduced Gröbner basis of $I^e = (Z_1 - 1, Z_2 - \frac{z_2}{z_1})$. One can check that $r(z_1, z_2) = r(1, \frac{z_2}{z_1})$ for any $r \in \mathbb{K}(z)^G = \mathbb{K}\left(\frac{z_2}{z_1}\right)$.

EXAMPLE 3.15 TRANSLATION+REFLECTION. Consider the group action from Example 2.4, 2.9, 2.18, 3.9. We chose the cross-section defined by $P = (Z_1 - Z_2)$ and found that $\mathbb{K}(z_2^2)$ was the field of rational invariants. Generic orbits have two components and the cross-section is of degree 2. Since $I^e = (Z_1 - Z_2, Z_2^2 - z_2^2)$, the two replacement invariants are $\xi^{(1)} = (z_2, z_2)$ and $\xi^{(2)} = (-z_2, -z_2)$. Though rational functions, their components are not rational invariants but only algebraic invariants.

EXAMPLE 3.16 ROTATION. Consider the group action from Example 2.5, 2.10, 2.19, 3.10. We chose the cross-section defined by $P = (Z_2)$. Here the cross-section is again of degree 2 but the generic orbits have a single component. Since $I^e = (Z_2, Z_1^2 - z_1^2 - z_2^2)$ the two replacement invariants associated to \mathcal{P} are $\xi^{(\pm)} = (0, \pm\rho)$ where ρ is the algebraic function defined by $\rho^2 = z_1^2 + z_2^2$.

4. Additional examples

We first consider a linear action of SL_2 on \mathbb{K}^7 considered by Derksen (1999). The latter presents an algorithm to compute a set of generators of the algebra of polynomial invariants for the linear action of a reductive group. The ideal of the graph $O = (G + (Z - g(\lambda, z))) \cap \mathbb{K}[z, Z]$, where now g is a polynomial map that is linear in z , is also central in Derksen's construction. A set of generators of $\mathbb{K}[z]^G$ is indeed obtained by applying the Reynolds operator, which is a projection from $\mathbb{K}[z]$ to $\mathbb{K}[z]^G$, to generators of $O + (Z_1, \dots, Z_n)$, the ideal of the null cone.

The fraction field of $\mathbb{K}[z]^G$ is included in $\mathbb{K}(z)^G$ but does not need to be equal. Conversely there is no known algorithm to compute $\mathbb{K}[z]^G = \mathbb{K}(z)^G \cap \mathbb{K}[z]$ from the knowledge of a set of generators of $\mathbb{K}(z)^G$.

EXAMPLE 4.1 We consider the linear action of SL_2 on \mathbb{K}^7 given by the following polynomials of $\mathbb{K}[\lambda_1, \dots, \lambda_4, z_1, \dots, z_7]$:

$$\begin{aligned} g_1 &= \lambda_1 z_1 + \lambda_2 z_2, & g_2 &= \lambda_3 z_1 + \lambda_4 z_2 \\ g_3 &= \lambda_1 z_3 + \lambda_2 z_4, & g_4 &= \lambda_3 z_3 + \lambda_4 z_4 \\ g_5 &= \lambda_1^2 z_5 + 2\lambda_1 \lambda_2 z_6 + \lambda_2^2 z_7, \\ g_6 &= \lambda_3 \lambda_1 z_5 + \lambda_1 \lambda_4 + \lambda_2 \lambda_3 z_6 + \lambda_2 \lambda_4 z_7, \\ g_7 &= \lambda_3^2 z_5 + 2\lambda_3 \lambda_4 z_6 + \lambda_4^2 \end{aligned}$$

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

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

By Theorem 3.7, $\mathbb{K}(z)^G = \mathbb{K}(r_1, r_2, r_3, r_4)$. In this case the rewriting of any rational invariant in terms of r_1, r_2, r_3, r_4 consists simply of the substitution of $(z_1, z_2, z_3, z_4, z_5, z_6, z_7)$ by $(-1, 0, 0, r_2, r_3, r_4, r_1)$. The latter tuple is the unique replacement invariant associated to the cross-section. We illustrate the replacement property by rewriting the five generating polynomial invariants computed by Derksen (1999) in terms of r_1, r_2, r_3, r_4 :

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

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

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

Though this Gröbner basis is obtained without much difficulty, the example illustrates the advantage obtained by considering the construction with a cross-section: I^e has a much simpler reduced Gröbner basis than O^e .

We finally take a classical example in differential geometry: the Euclidean action on the second order jets of plane curves. The variables x, y_0, y_1, y_2 stand for the independent variable, the dependent variable, first and the second derivatives respectively. We shall recognize the square of the curvature as the generating rational invariant. The curvature, like many other classical differential invariants, is an algebraic function of rational invariants. It appears in the replacement invariants.

EXAMPLE 4.2 We consider the group defined by $G = (\alpha^2 + \beta^2 - 1, \epsilon^2 - 1) \subset \mathbb{K}[\alpha, \beta, a, b, \epsilon]$. The neutral element is $(1, 0, 0, 0, 1)$, the group operation $(\alpha', \beta', a', b', \epsilon') \cdot (\alpha, \beta, a, b, \epsilon) = (\alpha\alpha' - \beta\beta', \beta\alpha' + \alpha\beta', a + \alpha a' - \beta b', b + \alpha a' + \alpha b', \epsilon \epsilon')$ and the inverse map $(\alpha, \beta, a, b)^{-1} = (\alpha, -\beta, -\alpha a - b\beta, \beta a - \alpha b, \epsilon)$. The rational action on \mathbb{K}^4 we consider is given by the rational functions:

$$\begin{aligned} g_1 &= \alpha x - \beta y_0 + a, & g_2 &= \epsilon \beta x + \epsilon \alpha y_0 + b, \\ g_3 &= \frac{\beta + \alpha y_1}{\alpha - \beta y_0}, & g_4 &= \frac{y_2}{(\alpha - \beta y_0)^3}. \end{aligned}$$

We have

$$O = \left((1 + y_1^2)^3 Y_2^2 - (1 + Y_1^2)^3 y_2^2 \right)$$

and if we consider the the cross section defined by $P = (X, Y_0, Y_1)$ the reduced Gröbner basis of $I^e = O^e + P$ is

$$\left\{ X, Y_0, Y_1, Y_2^2 - \frac{y_2^2}{(1 + y_1^2)^3} \right\}.$$

According to Theorem 2.16 or Theorem 3.7

$$\mathbb{K}(z)^G = \mathbb{K} \left(\frac{y_2^2}{(1 + y_1^2)^3} \right).$$

The Euclidean curvature appears as an element of the two replacement invariants $\xi^{(\pm)} = (0, 0, 0, \pm\sigma)$, where σ is the algebraic function defined by

$$\sigma^2 = \frac{y_2^2}{(1 + y_1^2)^3}.$$

For any rational invariant r we have the following equalities, by Theorem 3.13.

$$r(x, y_0, y_1, y_2) = r(0, 0, 0, \sigma) = r(0, 0, 0, -\sigma).$$

References

- Becker, T., Weispfenning, V., 1993. Gröbner Bases - A Computational Approach to Commutative Algebra. Springer-Verlag, New York.
- Cox, D., Little, J., O’Shea, D., 1992. Ideals, Varieties, and Algorithms. Springer-Verlag.
- Derksen, H., 1999. Computation of invariants for reductive groups. Adv. Math. 141 (2), 366–384.
- Derksen, H., Kemper, G., 2002. Computational invariant theory. Invariant Theory and Algebraic Transformation Groups, I. Springer-Verlag, Berlin, encyclopaedia of Mathematical Sciences, 130.
- Eisenbud, D., 1994. Commutative Algebra with a View toward Algebraic Geometry. Graduate Texts in Mathematics. Springer-Verlag New York.
- Fels, M., Olver, P. J., 1999. Moving coframes. II. Regularization and theoretical foundations. Acta Appl. Math. 55 (2), 127–208.
- Giusti, M., Heintz, J., 1993. La détermination des points isolés et de la dimension d’une variété algébrique peut se faire en temps polynomial. In: Computational algebraic geometry and commutative algebra (Cortona, 1991). Sympos. Math., XXXIV. Cambridge Univ. Press, Cambridge, pp. 216–256.
- Giusti, M., Heintz, J., Sabia, J., 1993. On the efficiency of effective Nullstellensätze. Computational Complexity 3 (1), 56–95.
- Greuel, G.-M., Pfister, G., 2002. A Singular introduction to commutative algebra. Springer-Verlag, Berlin.
- Hubert, E., Kogan, I. A., 2006. Smooth and algebraic invariants of a group action. Local and global construction. Submitted for publication.
- Krick, T., Pardo, L. M., Sombra, M., 2001. Sharp estimates for the arithmetic Nullstellensatz. Duke Mathematical Journal 109 (3), 521–598.

- Müller-Quade, J., Beth, T., 1999. Calculating generators for invariant fields of linear algebraic groups. In: Applied algebra, algebraic algorithms and error-correcting codes (Honolulu, HI, 1999). Vol. 1719 of Lecture Notes in Computer Science. Springer, Berlin, pp. 392–403.
- Müller-Quade, J., Steinwandt, R., 1999. Basic algorithms for rational function fields. *Journal of Symbolic Computation* 27 (2), 143–170.
- Rosenlicht, M., 1956. Some basic theorems on algebraic groups. *American Journal of Mathematics* 78, 401–443.
- Shafarevich, I. R., 1994. Basic algebraic geometry. 1, 2nd Edition. Springer-Verlag, Berlin, varieties in projective space, Translated from the 1988 Russian edition and with notes by Miles Reid.
- van der Waerden, 1971. Modern algebra, 8th Edition. Springer Verlag - New York.
- Vinberg, E. B., Popov, V. L., 1994. Invariant theory. In: Parshin, A., Shafarevich, I. R. (Eds.), Algebraic geometry. IV. Vol. 55 of Encyclopaedia of Mathematical Sciences. Springer-Verlag, Berlin, pp. 122–278.