Found. Comput. Math. 455–493 (2007)
© 2007 SFoCM
DOI: 10.1007/s10208-006-0219-0

FOUNDATIONS OF
COMPUTATIONAL
MATHEMATICS
The Journal of the Society for the Foundations of Computational Mathematics

Smooth and Algebraic Invariants of a Group Action: Local and Global Constructions

Evelyne Hubert[1] and Irina A. Kogan[2]

[1]INRIA Sophia Antipolis
2004 route des lucioles
06902 Sophia Antipolis
www.inria.fr/cafe/Evelyne.Hubert

[2]Department of Mathematics
North Carolina State University
245 Harrelson Hall
Campus Box 8205
Raleigh, NC 27695, USA
www.math.ncsu.edu/∼iakogan

Abstract. We provide an algebraic formulation of the moving frame method for constructing local smooth invariants on a manifold under an action of a Lie group. This formulation gives rise to algorithms for constructing rational and replacement invariants. The latter are algebraic over the field of rational invariants and play a role analogous to Cartan's normalized invariants in the smooth theory. The algebraic algorithms can be used for computing fundamental sets of differential invariants.

Introduction

Group actions are ubiquitous in mathematics and arise in diverse fields of science and engineering, including physics, mechanics, and computer vision. A central problem is to compute a generating set of invariants and the relations (syzygies)

Date received: January 30, 2006. Final version received: February 20, 2007. Date accepted: March 1, 2007. Communicated by Teresa Krik and Peter Olver. Online publication: June 14, 2007.
AMS classification: 13A50, 13P10, 14L24, 14Q99, 53A55.
Key words and phrases: Rational and algebraic invariants, Smooth and differential invariants, Algebraic and Lie group actions, Cross-section, Moving frame method, Gröbner basis.

among them. Algebraic invariant theory studies polynomial or rational invariants of algebraic group actions [**1], [17], [21], [41**]. A typical example is the discriminant of a binary form as an invariant of an action of the special linear group. The differential invariants appearing in differential geometry are smooth functions on a jet bundle that are invariant under a prolonged action of a Lie group. A typical example is the curvature of a plane curve, invariant under the action of the group of the isometries on the plane. Motivated by a wealth of applications,[1] both algebraic and differential invariant theories have become in recent years the subject of computational mathematics [**46**], [**12**], [**14**], [**10**], [**31**]. Differential invariants are intimately linked with physics and, more generally, with the study of differential systems, while algebraic theories give a proper setting to symbolic algorithms.

The ambition of our work is to provide algebraic foundations to the moving frame construction of differential invariants. The present paper deals with non-differential aspects of the moving frame construction so that we avoid the explicit introduction of jet bundles. We provide a novel presentation of the moving frame construction of Fels and Olver [**12**] for local smooth invariants (Section 1). It applies to a more general class of actions. For this presentation we can provide a parallel algebraic construction (Section 2) that produces algebraic invariants. Note that classical differential invariants, like curvatures, are algebraic functions and we use algebraic invariants accordingly. The parts concerning the smooth and local construction on one hand and the algebraic and global construction on the other hand can be read independently, one shedding light on the other. We then show that the algebraic setting offers a computational solution to the geometric construction (Section 3). Two geometrical examples illustrate the application of our algebraic approach to the computation of the fundamental set of well-known differential invariants (Section 4).

In the differential geometric approach we consider actions of Lie groups on smooth manifolds. We assume the action to be semiregular, i.e., that all orbits have the same dimension. We consider the class of locally smooth functions, i.e., functions which are smooth on some open subset of the manifold. The *local invariants* are locally smooth functions invariant with respect to transformations by the elements of the group close enough to the identity.

In the algebraic setting we consider rational actions of algebraic groups on an affine space. We consider rational and algebraic functions. *Algebraic invariants* are understood as elements that are algebraic over the field of rational invariants. To connect the smooth and the algebraic approaches we consider rational actions of real algebraic groups.

In both settings we construct tuples of invariants that have replacement properties and known relations on their components. The replacement property means that we can rewrite any other invariants in terms of the components of the tuple

[1] Here are a few references in different application fields that can serve as pointers: [**33**], [**34**], [**6**], [**14**], [**30**], [**4**], [**43**], [**38**], [**10**, Chap. 5].

by a simple substitution of the coordinate functions by the corresponding element of the tuple. This thus provides canonical representations for invariants. Both constructions rely on a choice of a cross-section to the orbits. The cross-section can be chosen with ample freedom, and it determines the relations on the constructed invariants. It is shown that invariants can be identified with the functions on the cross-section. The invariantization process is based on this identification. It is a projection from the set of functions to the set of invariant functions.

In the geometric approach (Section 1) we start by defining the invariantization process from the choice of a cross-section. We show that the local invariants can be identified with the functions on the cross-section. The invariantization of a function is then the local invariant that has the same restriction to the cross-section as the function. Invariantized coordinate functions are showed to have the replacement property, and to contain a fundamental set of invariants.

In the algebraic setting (Section 2) we start by defining the replacement invariants as tuples of algebraic invariants. They depend on the cross-section. They are the zeros of the *graph-section ideal*, i.e., the ideal of the intersection of a generic orbit with the cross-section. The graph-section ideal is proved to be prime when considered over the field of rational invariants. We can then deduce that the field of algebraic invariants is isomorphic to the field of algebraic functions on the cross-section. The isomorphism is computable by algebraic elimination. This is the basis of the invariantization process.

In Section 3 we show how algebraic invariantization, for which we provide an algorithm, gives a computational solution to smooth invariantization in the case of a rational action of a real algebraic group. This provides an explicit connection between Cartan's moving frame method for the construction of local invariants [**5**], [**20**], [**18**], [**12**], and the algebraic theory for rational invariants and the algorithms to compute them [**42], [41], [32], [23**].

We conclude the paper with two geometric examples (Section 4). They illustrate how a fundamental set of differential invariants can be computed using the algebraic algorithms presented in the paper. The actions of the Euclidean and affine groups on plane curves are investigated through the prolongation of the action on the plane to the jet bundle. The Euclidean and affine curvatures, which are algebraic functions, naturally arise in the replacement invariants for those actions.

Background for the Paper

Building on works [**20], [24], [18**], it was clearly established in [**12**] that Cartan's moving frame construction relies on a local group-equivariant map from a jet bundle to the group itself, and that Cartan's normalization procedure corresponds to choosing a local cross-section to the orbits.[2] A moving frame map defines an *invariantization process*. Invariantization of coordinate functions produces a *set of*

[2] This equivariant map is called *moving frame* in [**12**], and is called *moving frame map* in this paper.

normalized invariants, which contains a fundamental set. Moreover, any smooth invariant can locally be written in terms of the normalized invariants by a simple substitution. There are two main drawbacks associated with this construction. First, the local freeness[3] assumption on the group action is necessary for the existence of the moving frame map. Although this assumption is always satisfied on an open dense subset, when the action is prolonged to the jet bundle of sufficiently high order, it becomes an obstacle when one is interested only in the differential invariants of low order. Second, the proof of the existence of a local moving frame map relies on the implicit function theorem and is nonconstructive. The moving frame map might not be explicitly computable.

Both difficulties are circumvented in Section 1 by defining invariantization as a projection from the set of smooth functions onto the equivalence classes of functions with the same value on the cross-section. We give a constructive proof for the existence of a local coordinate cross-section through every point, provided the action is semiregular.[4] We show that in the case of locally free actions our definition of invariantization is equivalent to the definition in [**12**].

An application of the moving frame method to classical invariant theory [**1], [21], [46**] was proposed in [**37**], [**26**], [**3**], [**27**]. In these works, however, the geometric formulation of the method is used without adapting it to the algebraic nature of the problem. A purely algebraic formulation of the moving frame method opens new possibilities of its application in classical invariant theory.

Section 2 is an algebraic formulation of the moving frame construction. It can also be seen as a constructive counterpart to results in [**41**]. It is closely related to the constructions introduced in [**23**] to provide an algorithm for computing a generating set of rational invariants. The cross-sections that we introduce correspond to the quasi-sections in [**41**] and extend the notion of cross-section that appears in [**42**]. We indeed associate to a cross-section a *degree* that is the number of points of intersection with a generic orbit. Popov and Vinberg [**41**] show that the field of rational functions on the cross-section is an algebraic extension of degree d of the field of rational invariants. The field of algebraic functions on the cross-section is thus isomorphic to the field of algebraic invariants. We retrieve this result through the use of the replacement invariants. The new invariantization process provides a computational counterpart to this isomorphism. The replacement invariants furthermore provide a generating set of algebraic invariants with known relations among them and a canonical representation of algebraic invariants.

Differential invariants play a crucial role in solving a variety of problems in geometry and differential equations [**29], [39], [20], [13], [25], [36**]. The present paper is actually part of a bigger project, in the line of [**30], [22**], where the algebra of differential invariants and its application to differential elimination of symmetric differential systems is investigated.

[3] Local freeness means that the dimension of each orbit equals the dimension of the group.

[4] Semiregularity means that all orbits have the same dimension.

Outline of the Paper

In Section 1.1 we give a definition of a local action of a Lie group on a smooth manifold. In Section 1.2 we define local invariants and discuss the existence of a fundamental set of those. In Section 1.3 we show that a local cross-section passing through any given point can easily be constructed. In Section 1.4 we show that given a cross-section one can define an invariantization process, that is, a projection from the set of smooth functions to the set of local invariants. In Section 1.5 we show that invariantization provides a set of normalized invariants from which we extract a fundamental set of local invariants. In Section 1.6 we review the Fels–Olver invariantization process for free actions that is based on the moving frame map [**12**]. We show that our cross-section-based definition is equivalent.

In Section 2.1 we give a definition of a rational action of an algebraic group. Section 2.2 discusses rational and algebraic invariants. In Section 2.3 we introduce the graph of the action, the cross-section and the graph-section ideal. The replacement invariants are defined, in Section 2.4, as the zeros of this ideal. In Section 2.5 we prove that algebraic closure of the field of rational invariants is isomorphic to the field of algebraic functions on the cross-section. In Section 2.6 we use the replacement invariants to define an algebraic invariantization map that is computable by algebraic elimination.

In Section 3.1 we give an algebraic description of the moving frame map and argue in favor of the cross-section-based approach to smooth invariantization of Section 1.4 as an appropriate setting for algebraic algorithms. We prove that the normalized invariants of Section 1.5 are local smooth representatives of the elements of the replacement tuple of Section 3.2 and that algebraic invariantization provides a computational approach to smooth invariantization in Section 3.3.

In Section 4 we illustrate on classical examples how our algebraic construction can be used to compute differential invariants.

1. Local Invariants

We consider a local action of a Lie group on a smooth manifold and define local invariants. A fundamental set of invariants is defined as a minimal *functionally* generating set of invariants whose existence classically follows from the Frobenius theorem. We extend the notions of cross-section and invariantization of [**12**] to semiregular action. By basing the definition of invariantization directly on the cross-section alone we remove the necessity of a free action. Besides, that allows a reformulation in the algebraic context in Section 2. The invariantization process allows us to produce a set of normalized invariants which contains a fundamental set. Normalized invariants have the replacement property: any invariant can be written in terms of them by substitution of each coordinate function with the corresponding normalized invariant. We conclude this section by making an explicit comparison with the Fels–Olver moving frame construction [**12**].

In this section we consider real smooth manifolds. All statements and constructions from this section are applicable to complex manifolds. In the latter case all maps and functions are assumed to be meromorphic.

1.1. *Local Action of a Lie Group on a Smooth Manifold*

We consider a Lie group $\mathcal{G}$, with identity denoted by e and dimension κ, and a smooth manifold $\mathcal{Z}$ of dimension n. Points on $\mathcal{G}$ and $\mathcal{Z}$ are noted $\bar\lambda = (\bar\lambda_1, \dots, \bar\lambda_\kappa)$ and $\bar z = (\bar z_1, \dots, \bar z_n)$ while $\lambda = (\lambda_1, \dots, \lambda_\kappa)$ and $z = (z_1, \dots, z_n)$ denote the coordinate functions. We first review the necessary facts and terminology from the theory of Lie group actions on smooth manifolds. Our presentation is based on [**16**], [**35**].

Definition 1.1. A local action of a Lie group $\mathcal{G}$ on a smooth manifold $\mathcal{Z}$ is a smooth map $g : \Omega \to \mathcal{Z}$ where $\Omega \supset \{e\} \times \mathcal{Z}$ is an open subset of $\mathcal{G} \times \mathcal{Z}$ and g satisfies the following two properties:

1. $g(e, \bar z) = \bar z$ for all $\bar z \in \mathcal{Z}$.
2. $g(\bar\mu, g(\bar\lambda, \bar z)) = g(\bar\mu \cdot \bar\lambda, \bar z)$ for all $\bar z \in \mathcal{Z}$ and $\bar\lambda, \bar\mu \in \mathcal{G}$ s.t. $(\bar\lambda, \bar z)$ and $(\bar\mu \cdot \bar\lambda, \bar z)$ are in Ω.

The *orbit* of $\bar z \in \mathcal{Z}$ is the image $\mathcal{O}_{\bar z}$ of the smooth map $g_{\bar z} : \mathcal{G} \mapsto \mathcal{Z}$ defined by $g_{\bar z}(\bar\lambda) = g(\bar\lambda, \bar z)$. The domain of $g_{\bar z}$ is an open subset of $\mathcal{G}$ containing e.

For every point $\bar z \in \mathcal{Z}$ the differential $dg_{\bar z} : T\mathcal{G}|_e \to T\mathcal{Z}|_{\bar z}$ maps the tangent space of $\mathcal{G}$ at e to the tangent space of $\mathcal{Z}$ at the point $\bar z$. The tangent space $T\mathcal{G}|_e$ can be identified with the Lie algebra $\mathfrak{g}$ of $\mathcal{G}$. If $\hat v \in \mathfrak{g}$, then $v(\bar z) = dg_{\bar z}(\hat v)$ is a smooth vector field on $\mathcal{Z}$, called the *infinitesimal generator* of the $\mathcal{G}$-action corresponding to $\hat v$. The set of all infinitesimal generators for a $\mathcal{G}$-action form a Lie algebra, such that the map $\hat v \to v$ is a Lie algebra homomorphism.

By $\exp(\varepsilon v, \bar z) : \mathbb{R} \times \mathcal{Z} \to \mathcal{Z}$ we denote the flow of v. It is defined as the integral curve of the vector field v with initial condition $\bar z$. Every point of the connected component of the orbit $\mathcal{O}^0_{\bar z} \ni \bar z$ can be reached from $\bar z$ by a composition of flows of a finite number of infinitesimal generators.

Let $\hat v_1, \dots, \hat v_\kappa$ be a basis of the Lie algebra of $\mathcal{G}$. Then the infinitesimal generators $v_1, \dots, v_\kappa$ span the tangent space to the orbits at each point of $\mathcal{Z}$.

Definition 1.2. An action of a Lie group $\mathcal{G}$ on a smooth manifold $\mathcal{Z}$ is semiregular if all orbits have the same dimension.

Throughout this section the action is assumed to be semiregular. The dimension of the orbits is denoted by s.

1.2. *Local Invariants*

We give definitions of local invariants and fundamental sets of those. We discuss how the existence of a fundamental set of local invariants follows from the existence of a flat coordinate system.

Definition 1.3. A smooth function f, defined on an open subset $\mathcal{U} \subset \mathcal{Z}$, is a local invariant if $v(f) = 0$ for any infinitesimal generator v of the $\mathcal{G}$-action on $\mathcal{U}$.

Equivalently, $f(\exp(\varepsilon v, \bar{z})) = f(\bar{z})$ for all $\bar{z} \in \mathcal{U}$, all infinitesimal generators v, and all real ε sufficiently close to zero. If the group $\mathcal{G}$ is connected, the function f is continuous on $\mathcal{Z}$, and the condition of Definition 1.3 is satisfied at every point of $\mathcal{Z}$, then f is a global invariant on $\mathcal{Z}$ due to [**35**, Prop. 2.6]. In what follows we neither assume f to be continuous outside $\mathcal{U}$, nor $\mathcal{G}$ to be connected.

A collection of smooth functions $f_1, \dots, f_l$ are functionally *dependent* on a manifold $\mathcal{Z}$ if for each point $\bar{z} \in \mathcal{Z}$ there exists an open neighborhood $\mathcal{U}$ and a nonzero differentiable function F in l variables such that $F(f_1, \dots, f_l) = 0$ on $\mathcal{U}$. From the implicit function theorem it follows that $f_1, \dots, f_l$ are functionally dependent on $\mathcal{Z}$ if and only if the rank of the corresponding Jacobian matrix is less than l at each point of $\mathcal{Z}$. We say that functions $f_1, \dots, f_l$ are *independent* of $\mathcal{Z}$ if they are not dependent when restricted to any open subset of $\mathcal{Z}$. Equivalently, the corresponding Jacobian is nonzero on $\mathcal{Z}$ except, possibly, on a discrete set of points. As it is commented in [**35**, p. 85] functional dependence and functional independence on $\mathcal{Z}$ do not exhaust the range of possibilities, except for analytic functions. Throughout the section the term *independent functions* means *functionally independent functions*. Finally, we say that $f_1, \dots, f_l$ are independent at a point $\bar{z} \in \mathcal{Z}$ if the rank of the corresponding Jacobian matrix is maximal at $\bar{z}$. Independence at $\bar{z}$ implies independence on some open neighborhood of this point. If $\mathcal{U}$ is an open subset of $\mathcal{Z}$ and $f_1, \dots, f_n$ are independent at each point of $\mathcal{Z}$, then these functions provide a coordinate system on $\mathcal{U}$.

Definition 1.4. A collection of local invariants on $\mathcal{U}$ forms a *fundamental set* if they are functionally independent, and any local invariant on $\mathcal{U}$ can be expressed as a smooth function of the invariants from this set.

If the action is semiregular and the orbits are of dimension s, a fundamental set consists of $n - s$ local invariants. The proof of existence of a fundamental set of invariants relies on the following line of argument. The Lie algebra of infinitesimal generators provides an integrable distribution[5] of smooth vector fields on $\mathcal{Z}$, whose integral manifolds are connected components of the orbits. For a semiregular action

[5] An integrable distribution is a collection of smooth vector fields, whose span over the ring of smooth functions is closed with respect to the Lie bracket.

this distribution is of constant rank s, equal to the dimension of the orbits. It follows from the Frobenius theorem that on an open neighborhood $\mathcal{U}$ of each point there exists a coordinate system $x_1, \ldots, x_s, y_1, \ldots, y_{n-s}$ such that the connected components of the orbits on $\mathcal{U}$ are level sets of the last $n-s$ coordinates [**44**, p. 262] and [**35**, Theorem 1.43]. Such a coordinate system is called *flat, or straightening*. The coordinate functions $y_1, \ldots, y_{n-s}$ are thus local invariants. Using the fact that they are part of a coordinate system, one shows that they form a fundamental set (see, for instance, [**35**, Theorem 2.17]).

One can thus obtain a fundamental set by finding $n - s$ independent solutions for the system of linear, first-order partial differential equations $v_i(f) = 0$, $i = 1..\kappa$, where $v_1, \ldots, v_\kappa$ is a basis of infinitesimal generators. The invariantization process described in Section 1.4 provides an approach for obtaining a fundamental set of invariants that does not require integration. Invariantization and, therefore, fundamental sets of local invariants can effectively be computed either by the algorithms of Section 2.6, in the case of a rational action of an algebraic group (see Section 3), or by the moving frame method of [**12**], in the case of a locally free action of a Lie group (see Section 1.6).

1.3. *Local Cross-Section*

We define local cross-sections to the orbits. We show that a local cross-section passing through any given point can easily be constructed. As suggested in [**12**, Sect. 4], the definition and results are generalized to semiregular actions.

Definition 1.5. An embedded submanifold $\mathcal{P}$ of $\mathcal{Z}$ is a *local cross-section* to the orbits if there is an open set $\mathcal{U}$ of $\mathcal{Z}$ such that:

- $\mathcal{P}$ intersects $\mathcal{O}^0_{\bar{z}} \cap \mathcal{U}$ at a unique point for all $\bar{z} \in \mathcal{U}$, where $\mathcal{O}^0_{\bar{z}}$ is the connected component of $\mathcal{O}_{\bar{z}} \cap \mathcal{U}$, containing $\bar{z}$;
- for all $\bar{z} \in \mathcal{P} \cap \mathcal{U}$, $\mathcal{O}^0_{\bar{z}}$ and $\mathcal{P}$ are transversal and of complementary dimensions.

The second condition in the above definition is equivalent to the following condition on tangent spaces: $T_{\bar{z}}\mathcal{Z} = T_{\bar{z}}\mathcal{P} \oplus T_{\bar{z}}\mathcal{O}_{\bar{z}}$, for all $\bar{z} \in \mathcal{P} \cap \mathcal{U}$.

An embedded submanifold of codimension s can be locally defined as the zero set of s independent functions. Assume that $h_1(z), \ldots, h_s(z)$ define $\mathcal{P}$ on $\mathcal{U}$. The tangent space at a point of $\mathcal{P}$ is the kernel of the Jacobian matrix J_h at this point. As a basis of infinitesimal generators $v_1, \ldots, v_\kappa$ span the tangent space to the orbits at each point, the submanifold $\mathcal{P}$ is a local cross-section if and only if the span of $v_1, \ldots, v_\kappa$ has a trivial intersection with the kernel of J_h on $\mathcal{P}$. Equivalently,

$$\text{the rank of the } s \times \kappa \text{ matrix } \left(v_j(h_i)\right)_{i=1..s}^{j=1..\kappa} = J_h \cdot V \text{ equals } s \text{ on } \mathcal{P}, \qquad (1)$$

where V is the $n \times \kappa$ matrix, whose ith column consists of the coefficients of the infinitesimal generator v_i in a local coordinate system. In the next theorem we prove the existence of a local cross-section through every point. The first paragraph of the proof provides a simple practical algorithm to construct a coordinate local cross-section through a point.

Theorem 1.6. *Let $\mathcal{G}$ act semiregularly on $\mathcal{Z}$. Through every point $\bar{z} \in \mathcal{Z}$ there is a local cross-section that is defined as the level set of s coordinate functions.*

Proof. Let V be the $n \times \kappa$ matrix of the coefficients of the infinitesimal generators $v_1, \dots, v_\kappa$ relative to a coordinate system $z_1, \dots, z_n$. The rank of V equals the dimension of the orbits s. Thus there exist s rows of V that form an $s \times \kappa$ submatrix $\hat{V}$ of rank s at the point $\bar{z}$ and, therefore, it has rank s on an open neighborhood $\mathcal{U}_1 \ni \bar{z}$. Assume that these rows correspond to coordinates $z_{i_1}, \dots, z_{i_s}$. Let $(c_1, \dots, c_n)$ be coordinates of the point $\bar{z}$, then functions $h_1 = z_{i_1} - c_{i_1}, \dots, h_s = z_{i_s} - c_{i_s}$ satisfy condition (1). The common zero set $\mathcal{P}$ of these functions contains $\bar{z}$.

It remains to prove that there exists a neighborhood $\mathcal{U} \ni \bar{z}$ such that $\mathcal{P}$ intersects each connected component of the orbits on $\mathcal{U}$ at a unique point. Let $x_1, \dots, x_s, y_1, \dots, y_{n-s}$ be a flat coordinate system in an open neighborhood $\mathcal{U}_2 \ni \bar{z}$. Due to [**35**, Theorem 2.17] $y_1, \dots, y_{n-s}$ are independent local invariants. We will show that functions $z_{i_1}, \dots, z_{i_s}, y_1, \dots, y_{n-s}$ provide a coordinate system, an open set $\mathcal{U} = \mathcal{U}_1 \cap \mathcal{U}_2$ containing $\bar{z}$. Without loss of generality we may assume that $\{z_{i_1}, \dots, z_{i_s}\} = \{z_1, \dots, z_s\}$ are the first s coordinates. In terms of flat coordinates $z_i = F_i(x, y),\ i = 1..s$, where F_i are smooth functions on $\mathcal{U}_2$. Since $v_i(y_j) = 0$ for $i = 1..\kappa,\ j = 1..n - s$, then

$$(v_j(z_i))_{i=1..s}^{j=1..\kappa} = \left(\frac{\partial F_i}{\partial x_r}\right)_{i=1..s}^{r=1..s} \cdot (v_j(x_r))_{r=1..s}^{j=1..\kappa}. \tag{2}$$

We note that $(v_i(z_j))_{j=1..s}^{i=1..\kappa} = \hat{V}$ is $s \times \kappa$ matrix of rank s at each point of $\mathcal{U}$. Matrix $(v_j(x_r))_{r=1..s}^{j=1..\kappa}$ also has maximal rank s on $\mathcal{U}$. Therefore the matrix $(\partial F_i/\partial x_r)_{i=1..s}^{r=1..s}$ is invertible on $\mathcal{U}$. By looking at the rank of the corresponding Jacobian matrix in flat coordinates, we conclude that functions $z_1, \dots, z_s, y_1, \dots, y_{n-s}$ are independent at each point of $\mathcal{U}$, and therefore define a coordinate system on $\mathcal{U}$.

By construction, all points on $\mathcal{P}$ have the same z-coordinates. Thus two distinct points of $\mathcal{P}$ must differ by at least one of the y-coordinates. Since y coordinates are constant on the connected components of the orbits on $\mathcal{U}$, distinct points of $\mathcal{P}$ belong to distinct connected components of the orbits. □

1.4. *Invariants as Smooth Functions on the Cross-Section*

As introduced in [**12**], an *invariantization process* is a projection from the set of smooth functions on $\mathcal{U}$ to the set of local invariants. A cross-section on $\mathcal{U}$ defines an invariantization process: a local cross-section defines equivalence relationship on the ring of smooth functions any class of which has a single representative that is a local invariant. The present definition of the invariantization process differs from the one in [**12**] in that it depends directly on the cross-section and, consequently, does not require the action to be free.

Definition 1.7. Let $\mathcal{P}$ be a local cross-section to the orbits on an open set $\mathcal{U}$. Let f be a smooth function on $\mathcal{U}$. The *invariantization* $\bar{\iota} f$ of f is the function on $\mathcal{U}$ that is defined by $\bar{\iota} f(\bar{z}) = f(\bar{z}_0)$ for each $\bar{z} \in \mathcal{U}$, where $\bar{z}_0 = \mathcal{O}^0_{\bar{z}} \cap \mathcal{P}$.

In other words, the invariantization of a function f is obtained by spreading the values of f on $\mathcal{P}$ along the orbits. The next theorem shows that $\bar{\iota} f$ is the unique local invariant with the same values on $\mathcal{P}$ as f.

Theorem 1.8. *Let a Lie group $\mathcal{G}$ act semiregularly on a manifold $\mathcal{Z}$, and let $\mathcal{P}$ be a local cross-section. Then $\bar{\iota} f$ is the unique local invariant defined on $\mathcal{U}$ whose restriction to $\mathcal{P}$ is equal to the restriction of f to $\mathcal{P}$. In other words, $\bar{\iota} f|_{\mathcal{P}} = f|_{\mathcal{P}}$.*

Proof. For any $\bar{z} \in \mathcal{U}$ and small enough ε the point $\exp(\varepsilon v, \bar{z})$ belongs to the same connected component $\mathcal{O}^0_{\bar{z}}$. Let $\bar{z}_0 = \mathcal{O}^0_{\bar{z}} \cap \mathcal{P}$. Then $\bar{\iota} f(\exp(\varepsilon v, \bar{z})) = f(\bar{z}_0) = \bar{\iota} f(\bar{z})$, and thus $\bar{\iota} f$ is a local invariant. By definition $\bar{\iota} f(\bar{z}_0) = f(\bar{z}_0)$ for all $\bar{z}_0 \in \mathcal{P}$.

In order to show its smoothness we write $\bar{\iota} f$ in terms of flat coordinates $x_1, \ldots, x_s, y_1, \ldots, y_{n-s}$. By probably shrinking $\mathcal{U}$, we may assume that $\mathcal{P}$ is given by the zero-set of smooth independent functions $h_1(x_1, \ldots, x_s, y_1, \ldots, y_{n-s}), \ldots, h_s(x_1, \ldots, x_s, y_1, \ldots, y_{n-s})$. From the transversality condition (1) and local invariance of y's, it follows that the first s columns of the Jacobian matrix J_h form a submatrix of rank s. Thus the cross-section $\mathcal{P}$ can be described as a graph $x_1 = p_1(y_1, \ldots, y_{n-s}), \ldots, x_s = p_s(y_1, \ldots, y_{n-s})$, where $p_1, \ldots, p_s$ are smooth functions. Then the function

$$\begin{aligned}\bar{\iota} f&(x_1, \ldots, x_s, y_1, \ldots, y_{n-s})\\ &= f\left(p_1(y_1, \ldots, y_{n-s}), \ldots, p_s(y_1, \ldots, y_{n-s}), y_1, \ldots, y_{n-s}\right)\end{aligned}$$

is smooth, as a composition of smooth functions.

To prove the uniqueness, assume that an invariant function q has the same values on $\mathcal{P}$ as f, then the invariant function $h = \bar{\iota} f - q$ has zero value on $\mathcal{P}$. A point $\bar{z} \in \mathcal{U}$ can be reached from $\bar{z}_0 = \mathcal{P} \cap \mathcal{O}^0_{\bar{z}}$ by a composition of flows defined by infinitesimal generators. Without loss of generality, we may assume that it can be reached by a single flow $\bar{z} = \exp(\varepsilon v, \bar{z}_0)$, where $\exp(\varepsilon v, \bar{z}_0) \subset \mathcal{O}^0_{\bar{z}}$ for all $0 \leq \varepsilon \leq \varepsilon$. From the invariance of h it follows that $h(\exp(\varepsilon v, \bar{z}_0)) = h(\bar{z}_0) = 0$. Thus $q(z) = \bar{\iota} f(z)$ on $\mathcal{U}$. □

Theorem 1.8 allows us to view the invariantization process as a projection from the set of smooth functions on $\mathcal{U}$ to the equivalence classes of functions with the same value on $\mathcal{P}$. Each equivalence class contains a unique local invariant. The algebraic counterpart of this point of view is described in Section 2.6.

The invariantization of differential forms can be defined in a similar implicit manner. It has been shown in [**12**], [**28**] that the essential information about the differential ring of invariants and the structure of differential forms can be computed from the infinitesimal generators of the action and the equations that define the cross-section, without explicit formulas for invariants.

1.5. *Normalized and Fundamental Invariants*

The *normalized invariants* are defined in [**12**] as the invariantizations of the coordinate functions. They are proved to have the replacement property: every invariant can be rewritten in terms of them by substituting coordinates functions by the corresponding invariants. Since our definition of invariantization differs from [**12**] we restate and prove the replacement theorem. We then show that a set of normalized invariants contains a fundamental set of local invariants.

In the algebraic context the set of normalized invariants corresponds to a *replacement* invariant defined in Section 2.6. This correspondence is made precise by Proposition 3.6.

All results of this subsection are stated under the following assumptions. The manifold $\mathcal{P}$ is a local cross-section to the s-dimensional orbits of a semiregular $\mathcal{G}$-action on an open $\mathcal{U} \subset \mathcal{Z}$. The corresponding invariantization map is $\bar{\iota}$. The set $\mathcal{U}$ is a single coordinate chart on $\mathcal{Z}$ with coordinate functions $z_1, \ldots, z_n$. By possibly shrinking $\mathcal{U}$ we may assume that $\mathcal{P}$ is the zero-set of s independent smooth functions.

Theorem 1.9. *If $f(z_1, \ldots, z_n)$ is a local invariant on $\mathcal{U}$, then $f(\bar{\iota}z_1, \ldots, \bar{\iota}z_n) = f(z_1, \ldots, z_n)$.*

Proof. Since $\bar{\iota}z_1|_{\mathcal{P}} = z_1|_{\mathcal{P}}, \ldots, \bar{\iota}z_n|_{\mathcal{P}} = z_n|_{\mathcal{P}}$, then $f(\bar{\iota}z_1, \ldots, \bar{\iota}z_n)|_{\mathcal{P}} = f(z_1, \ldots, z_n)|_{\mathcal{P}}$. Thus functions $f(\bar{\iota}z_1, \ldots, \bar{\iota}z_n)$ and $f(z_1, \ldots, z_n)$ are both local invariants and have the same value on $\mathcal{P}$. By Theorem 1.8 they coincide. □

Lemma 1.10. *Let $\mathcal{P}$ be a local cross-section on $\mathcal{U}$, given as the zero-set of s independent functions $h_1, \ldots, h_s$. Then $h_1(\bar{\iota}z_1, \ldots, \bar{\iota}z_n) = 0, \ldots, h_s(\bar{\iota}z_1, \ldots, \bar{\iota}z_n) = 0$ on $\mathcal{U}$. If, for a differentiable n-variable function f, we have $f(\bar{\iota}z_1, \ldots, \bar{\iota}z_n) \equiv 0$ on an open subset of $\mathcal{U}$, then there exists an open set $\mathcal{W} \subset \mathcal{U}$ such that $\mathcal{W} \cap \mathcal{P} \neq \emptyset$ and at each point of $\mathcal{W} \cap \mathcal{P}$ the functions $f, h_1, \ldots, h_s$ are not independent.*

Proof. Since $h(\bar{\iota}z)|_{\mathcal{P}} = \bar{\iota}h(z)|_{\mathcal{P}}$ and both functions are invariants, one has $h(\bar{\iota}z) = \bar{\iota}h(z)$ by Theorem 1.8. The latter is zero since $h|_{\mathcal{P}} = 0$. Assume now that there exits a differentiable function f and an open subset of $\mathcal{V} \subset \mathcal{U}$ such that $f(\bar{\iota}z_1, \ldots, \bar{\iota}z_n) \equiv 0$ on $\mathcal{V}$. Then $f(\bar{\iota}z_1, \ldots, \bar{\iota}z_n) \equiv 0$ at every point obtained from point in $\mathcal{V}$ by the cation of an element in $\mathcal{G}$. Thus there exists an open $\mathcal{W} \supset \mathcal{V}$ such that $f(\bar{\iota}z_1, \ldots, \bar{\iota}z_n) \equiv 0$ on $\mathcal{W}$ and $\mathcal{W} \cap \mathcal{P} \neq \emptyset$. We conclude that

$f(z_1, \ldots, z_n) \equiv 0$ on $\mathcal{P} \cap \mathcal{W}$. In this case f cannot be independent of $h_1, \ldots, h_s$ at any point of $\mathcal{P} \cap W$ since, otherwise, this would imply that $\mathcal{P}$ is of dimension less than $n - s$. □

Theorem 1.11. *Let $\mathcal{P}$ be a local cross-section on $\mathcal{U}$. The set $\{\bar{\iota}z_1, \ldots, \bar{\iota}z_n\}$ of the invariantizations of the coordinate functions $z_1, \ldots, z_n$ contains a fundamental set of $n - s$ local invariants on $\mathcal{U}$.*

Proof. Due to the implicit function theorem, after a possible shrinking $\mathcal{U}$ and renumbering of the coordinate functions, we may assume that $\mathcal{P}$ is the zero-set of the functions $h_1(z) = z_1 - p_1(z_{s+1}, \ldots, z_n), \ldots, h_s(z) = z_s - p_s(z_{s+1}, \ldots, z_n)$. Therefore $\bar{\iota}z_1 = p_1(\bar{\iota}z_{s+1}, \ldots, \bar{\iota}z_n), \ldots, \bar{\iota}z_s = p_k(\bar{\iota}z_{s+1}, \ldots, \bar{\iota}z_n)$ by Theorem 1.8. From Theorem 1.9 we can conclude that any local invariant can be written in terms of $\bar{\iota}z_{s+1}, \ldots, \bar{\iota}z_n$. For every differentiable nonzero $(n-s)$-variable function f, the functions $f(z_{s+1}, \ldots, z_n), h_1(z), \ldots, h_s(z)$ are independent at every point of $\mathcal{U}$. By Lemma 1.10, $\bar{\iota}z_{s+1}, \ldots, \bar{\iota}z_n$ are thus functionally independent on $\mathcal{U}$. □

Example 1.12 (Rotation). We consider the linear action of $SO(2)$, the group of 2×2 orthogonal matrices with determinant 1, on $\mathbb{R}^2$. The action of an element of the group is a rotation with the origin as center. The orbits are the circles centered at the origin, and the origin itself. The action is thus semiregular on $\mathcal{Z} = \mathbb{R}^2 \backslash \{(0, 0)\}$.

The positive z_1-axis, $\mathcal{P} = \{(z_1, z_2) | z_2 = 0, z_1 > 0\}$, is a local cross-section on $\mathcal{Z}$. The invariantization of the coordinate functions are the functions $\bar{\iota}z_1$ and $\bar{\iota}z_2$ that associate to a point $(\bar{z}_1, \bar{z}_2)$ the coordinates of the intersection of its orbit with the cross-section. Thus

$$\bar{\iota}z_1 : (z_1, z_2) \mapsto \sqrt{z_1^2 + z_2^2} \qquad \text{and} \qquad \bar{\iota}z_2 : (z_1, z_2) \mapsto 0.$$

By Theorem 1.11, all local invariants can be written in terms of $\sqrt{z_1^2 + z_2^2}$.

Example 1.13 (Translation + reflection). We next consider the direct product of the additive group $\mathbb{R}$ with the two-element group $\{-1, 1\}$. This is a one-dimensional Lie group with two connected components.

We take its action on the plane as translation parallel to the first coordinate axis and reflection with respect to this axis. It is defined by

$$\begin{aligned} g : (\mathbb{R} \times \{-1, 1\}) \times \mathbb{R}^2 &\rightarrow \mathbb{R}^2, \\ ((\lambda_1, \lambda_2), (z_1, z_2)) &\mapsto (z_1 + \lambda_1, \lambda_2 z_2). \end{aligned}$$

The action is semiregular on $\mathcal{Z} = \mathbb{R}^2$. The z_1-axis is an orbit and outside it the orbits have two components consisting of two straight lines parallel to the z_1-axis.

For any smooth function $h : \mathbb{R} \rightarrow \mathbb{R}$ the manifold $\mathcal{P} = \{(h(z_2), z_2) \mid z_2 \in \mathbb{R}\}$ is a local cross-section on $\mathcal{Z}$: it intersects each connected component of an orbit once.

More precisely, the point of intersection of the cross-section and the connected component of the orbit containing $(\bar{z}_1, \bar{z}_2)$ is $(h(\bar{z}_2), \bar{z}_2)$. Therefore,

$$\bar{\iota} z_1 : (z_1, z_2) \mapsto h(z_2) \qquad \text{and} \qquad \bar{\iota} z_2 : (z_1, z_2) \mapsto z_2.$$

According to Theorem 1.9, any local invariant $f : \mathcal{Z} \to \mathbb{R}$ thus satisfies $f(z_1, z_2) = f(h(z_2), z_2)$. We can conclude here that f does not depend on z_1. Note that z_2 is invariant under the action of the connected component of the group that contains the identity and, therefore, is a local invariant of the group action. It is not a global invariant, however, as it is not invariant under the action of the entire group.

The previous two examples illustrate that computing normalized invariants amounts to finding the intersections point of a generic orbit with the cross-section. The approach introduced in [**12**] and reproduced in the next section allows us to do this in a systematic manner.

1.6. *Moving Frame Map*

We show that the invariantization map described in Section 2.6 extends the invariantization process described in [**12**] to the case of nonfree semiregular actions. The latter is based on a local $\mathcal{G}$-equivariant map $\rho : \mathcal{U} \to \mathcal{G}$ from an open subset $\mathcal{U} \subset \mathcal{Z}$ to an open neighborhood of $e \in \mathcal{G}$. If the action is locally free the existence of ρ is proved by the implicit function theorem. This theorem is not constructive and, therefore, the map might not be explicitly computable. We review the Fels–Olver construction, and prove that in the case of locally free actions it is equivalent to the one presented in Section 1.3.

Definition 1.14. An action of a Lie group $\mathcal{G}$ on a manifold $\mathcal{Z}$ is *locally free* if for every point $\bar{z} \in \mathcal{Z}$ its isotropy group $\mathcal{G}_{\bar{z}} = \{\bar{\lambda} \in \mathcal{G} \mid \bar{\lambda} \cdot \bar{z} = \bar{z}\}$ is discrete.

Local freeness implies semiregularity of the action with the dimension of each orbit being equal to the dimension of the group. Theorem 4.4 from [**12**] can be restated as follows.

Theorem 1.15. *A Lie group $\mathcal{G}$ acts locally freely on $\mathcal{Z}$ if and only if every point of $\mathcal{Z}$ has an open neighborhood $\mathcal{U}$ such that there exists a map $\rho : \mathcal{U} \to \mathcal{G}$ that makes the following diagram commute. Here the map $\bar{\mu} \mapsto \bar{\mu} \cdot \bar{\lambda}^{-1}$ is chosen for the action of $\mathcal{G}$ on itself, and $\bar{\lambda}$ is taken in a suitable neighborhood (depending on the point of $\mathcal{U}$) of the identity in $\mathcal{G}$,*

$$\begin{tikzcd}
\mathcal{U}_\rho \arrow[r, "\bar{\lambda}"] \arrow[d] & \mathcal{U} \arrow[d, "\rho"] \\
\mathcal{G}_{\bar{\lambda}} \arrow[r] & \mathcal{G}
\end{tikzcd}$$

The map ρ is locally $\mathcal{G}$-equivariant, that is, $\rho(\bar{\lambda} \cdot \bar{z}) = \rho \cdot \bar{\lambda}^{-1}$ for $\bar{\lambda}$ sufficiently close to the identity, and is called *a moving frame map*. If $\mathcal{P}$ is a local cross-section, then the equation

$$\rho(\bar{z}) \cdot \bar{z} \in \mathcal{P} \tag{3}$$

uniquely defines $\rho(\bar{z})$ in a sufficiently small neighborhood of the identity. In particular, $\rho(\bar{z}_0) = e$ for all $\bar{z}_0 \in \mathcal{P}$. Reciprocally, a moving frame map defines a local cross-section to the orbits: $\mathcal{P} = \{\rho(\bar{z}) \cdot \bar{z} \mid \bar{z} \in \mathcal{U}\}$.

In local coordinates, condition (3) provides implicit equations for expressing the group parameters in terms of the coordinate functions on the manifold. The local existence of smooth solutions is guaranteed by the transversality condition and the implicit function theorem when the group acts locally freely. Since the implicit function theorem is not constructive, we might nonetheless not be able to obtain explicit formulas for the moving frame map.

In [**12**, Def. 4.6] the invariantization of a function f on $\mathcal{U}$ is defined as the function whose value at a point $\bar{z} \in \mathcal{U}$ is equal to $f(\rho(\bar{z}) \cdot \bar{z})$. The next proposition shows that this definition of invariantization based on a moving frame map is equivalent to Definition 1.7 given in terms of a cross-section. The advantage of the latter definition is that it is not restricted to locally free actions.

Proposition 1.16. *Let ρ be a moving frame map on $\mathcal{U}$. Then*

$$\bar{\iota} f(\bar{z}) = f(\rho(\bar{z}) \cdot \bar{z}).$$

Proof. Local invariance of $f(\rho(z) \cdot z)$ follows from the local equivariance of ρ, i.e., for $\bar{\lambda}$ sufficiently close to the identity,

$$f(\rho(\bar{\lambda} \cdot \bar{z}) \cdot (\bar{\lambda} \cdot \bar{z})) = f(\rho(\bar{z})\bar{\lambda}^{-1} \cdot (\bar{\lambda} \cdot \bar{z})) = f(\rho(\bar{z}) \cdot \bar{z}).$$

Since $\rho(z_0) = e$, then $f(\rho(\bar{z}_0) \cdot \bar{z}_0) = f(\bar{z}_0)$ for all $\bar{z}_0 \in \mathcal{P}$. Thus $f(\rho(z) \cdot z)$ is locally invariant and equals f, when restricted to $\mathcal{P}$. The conclusion follows from Theorem 1.8. □

Example 1.17 (Rotation). We consider again the linear action of $SO(2)$ described in Example 1.12. A group element acts as a rotation in the plane with the origin as center. The positive z_1-axis, $\mathcal{P} = \{(\bar{z}_1, \bar{z}_2) \mid z_2 = 0, z_1 > 0\}$, is a local cross-section on $\mathcal{Z} = \mathbb{R}^2 \setminus \{(0, 0)\}$. The associated moving frame map ρ takes a point $(\bar{z}_1, \bar{z}_2)$ to the element of the group whose action is the rotation that brings $(\bar{z}_1, \bar{z}_2)$ to the positive z_1-axis. We described already in Example 1.12 the resulting normalized invariants.

In general though, when the geometry of the orbits is not simple, one relies on a local parametrization of the group. Condition (3) can then be expressed in terms of equations which are meant to be solved for the group parameters.

More precisely, if $\varphi : \Omega \subset \mathcal{G} \to \mathbb{R}^s$ is a coordinate system on Ω, an open set of $\mathcal{G}$ that contains e, we introduce, often tacitly,

$$\tilde{\rho} = \varphi \circ \rho : \mathcal{U} \to \mathbb{R}^s,$$

where the open set $\mathcal{U}$ is contained in the domain of definition of ρ. If the local cross-section $\mathcal{P}$ is defined on $\mathcal{U}$ as the zero-set of the independent smooth functions $h_1, \ldots, h_s$, then (3) translates into equations

$$h_1(g(\varphi^{-1}(\tilde{\rho}(z)),\, z)) = 0,\ \ldots,\ h_s(g(\varphi^{-1}(\tilde{\rho}(z)),\, z)) = 0.$$

Example 1.18 (Rotation). We resume Example 1.12 using the usual local parametrization of $SO(2)$,

$$\begin{aligned} \varphi^{-1} :]{-\pi}, \pi[\ &\to\ SO(2)\backslash\{-Id\}, \\ \theta\ &\mapsto\ \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}. \end{aligned}$$

Then (3) becomes $z_1 \sin\theta + z_2 \cos\theta = 0$. Taking in account that $z_1 \cos\theta - z_2 \sin\theta > 0$, we obtain

$$\tilde{\rho}(z_1, z_2) = \begin{cases} -\tan^{-1}\left(\dfrac{z_2}{z_1}\right) & \text{for } z_1 > 0, \\ -\pi/2 & \text{for } z_1 = 0,\ z_2 > 0, \\ -\pi - \tan^{-1}\left(\dfrac{z_2}{z_1}\right) & \text{for } z_1 < 0, z_2 > 0, \\ \pi/2 & \text{for } z_1 = 0,\ z_2 < 0, \\ \pi - \tan^{-1}\left(\dfrac{z_2}{z_1}\right) & \text{for } z_1 < 0, z_2 < 0. \end{cases}$$

In Section 3 we provide an algebraic approach to invariantization that applies to rational actions. This example falls into this category if we consider the rational parametrization of $SO(2)$:

$$\begin{aligned} \varphi^{-1} : \mathbb{R}\ &\to\ SO(2)\backslash\,\{-Id\}\,, \\ t\ &\mapsto\ \begin{pmatrix} \dfrac{1-t^2}{1+t^2} & -\dfrac{2t}{1+t^2} \\ \dfrac{2t}{1+t^2} & \dfrac{1-t^2}{1+t^2} \end{pmatrix}. \end{aligned}$$

Then

$$\tilde{\rho}(z_1, z_2) = \begin{cases} 0 & \text{when } z_2 = 0 \text{ and } z_1 > 0, \\ \dfrac{z_1 - \sqrt{z_1^2 + z_2^2}}{z_2} & \text{when } z_2 \neq 0. \end{cases}$$

In both cases the domain of definition of $\tilde{\rho}$ is $\mathcal{Z}\backslash\{(z_1, 0) \mid z_1 < 0\}$ while the domain of definition of ρ is $\mathcal{Z}$. Its expression is

$$\rho(z_1, z_2) = \begin{pmatrix} \dfrac{z_1}{\sqrt{z_1^2+z_2^2}} & \dfrac{z_2}{\sqrt{z_1^2+z_2^2}} \\ -\dfrac{z_2}{\sqrt{z_1^2+z_2^2}} & \dfrac{z_1}{\sqrt{z_1^2+z_2^2}} \end{pmatrix}.$$

From $(\bar{\iota}z_1, \bar{\iota}z_2) = \rho(z) \cdot z$ we retrieve

$$\bar{\iota}z_1 : (z_1, z_2) \mapsto \sqrt{z_1^2+z_2^2} \qquad \text{and} \qquad \bar{\iota}z_2 : (z_1, z_2) \mapsto 0.$$

Example 1.19 (Scaling). We consider the scaling action of the multiplicative group $\mathbb{R}^*$ on $\mathbb{R}^2$,

$$\begin{aligned} g : \mathbb{R}^* \times \mathbb{R}^2 &\to \mathbb{R}^2, \\ (\lambda, z_1, z_2) &\mapsto (\lambda z_1, \lambda z_2). \end{aligned}$$

The orbits consist of the punctured straight lines through the origin and the origin itself. The action is free on $\mathcal{Z} = \mathbb{R}^2\backslash\{(0, 0)\}$.

The manifold $\mathcal{P} = \{(1, z_2) \mid z_2 \in \mathbb{R}\} \subset \mathbb{R}^2$ intersects each orbit of $\mathcal{U} = \mathcal{Z}\backslash\{(0, z_2) \mid z_2 \in \mathbb{R}\}$ once. It is a local cross-section on $\mathcal{U}$. Condition (3) becomes $\lambda z_1 = 1$ and leads to the associated moving frame map

$$\begin{aligned} \rho : \mathcal{U} &\to \mathbb{R}^*, \\ (z_1, z_2) &\mapsto \frac{1}{z_1}. \end{aligned}$$

The normalized invariants, i.e., the invariantizations of the coordinate functions, are thus

$$(\bar{\iota}z_1, \bar{\iota}z_2) = g\left(\rho(z_1, z_2), (z_1, z_2)\right) = \left(1, \frac{z_2}{z_1}\right).$$

The invariantization of a function f on $\mathcal{U}$ is defined by $\bar{\iota} f(z_1, z_2) = f(1, z_2/z_1)$. In agreement with Theorem 1.8, $\bar{\iota} f$ is the unique smooth function that agrees with f on $\mathcal{P}$. In particular, for any local invariant f, $f(z_1, z_2) = f(1, z_2/z_1)$.

If one is interested in having a local cross-section on the whole of $\mathcal{Z}$ we can consider the unit circle $\mathcal{P} = \{(z_1, z_2) \in \mathcal{Z} \mid z_1^2 + z_2^2 = 1\}$. It intersects each orbit of $\mathcal{Z}$ twice, but only once each connected component. Condition (3) becomes $\lambda^2(z_1^2 + z_2^2) = 1$. We have to choose the connected component of the identity in $\mathcal{G}$ as the image of the moving frame map

$$\begin{aligned} \rho : \mathcal{Z} &\to \mathbb{R}^*_{>0}, \\ (z_1, z_2) &\mapsto \frac{1}{\sqrt{z_1^2+z_2^2}}. \end{aligned}$$

The resulting normalized invariants are defined everywhere on $\mathcal{Z}$, yet are invariant only under the action of $\mathbb{R}^*_{>0}$, the connected component of identity in the group

$$(\bar{\iota}z_1, \bar{\iota}z_2) = \left(\frac{z_1}{\sqrt{z_1^2 + z_2^2}}, \frac{z_2}{\sqrt{z_1^2 + z_2^2}} \right).$$

Example 1.20 (Translation + reflection). We resume Example 1.13 where we considered the action of the direct product of the additive group $\mathbb{R}$ with the two-element group $\{-1, 1\}$ defined by

$$\begin{aligned} g : (\mathbb{R} \times \{-1, 1\}) \times \mathbb{R}^2 &\rightarrow \mathbb{R}^2, \\ ((\lambda_1, \lambda_2), (z_1, z_2)) &\mapsto (z_1 + \lambda_1, \lambda_2 z_2). \end{aligned}$$

Outside the z_1-axis, the orbits have two connected components. For any smooth function $h : \mathbb{R} \rightarrow \mathbb{R}$ the manifold $\mathcal{P} = \{(h(z_2), z_2) \mid z_2 \in \mathbb{R}\}$ is a local cross-section on $\mathcal{Z}$.

Condition (3) becomes $z_1 + \lambda_1 = h(\lambda_2 z_2)$, and provides the moving frame map defined by

$$\rho(z_1, z_2) = (h(z_2) - z_1, 1),$$

which takes its values in the connected component $\mathbb{R} \times \{1\}$ of the identity in $\mathcal{G}$.

By Proposition 1.16 the normalized invariants are

$$(\bar{\iota}z_1, \bar{\iota}z_2) = g(\rho(z_1, z_2), (z_1, z_2)) = (h(z_2), z_2).$$

In agreement with Theorem 1.8, $\bar{\iota}z_1 = h(z_2)$ and $\bar{\iota}z_2 = z_2$ are the unique smooth local invariants that agree with z_1 and z_2 on $\mathcal{P}$.

The coordinate function z_2 is a local invariant (Definition 1.3) and all local invariants can be written as smooth functions of z_2 (Theorem 1.9). Note though that it is not invariant under the full group.

Thus the moving frame map offers an approach to invariantization that is constructive up to the resolution of the implicit equations given by (3). We provide an algebraic formulation of the moving frame map in Section 3.1. If one can obtain the map ρ explicitly, the invariantization map can be computed using Proposition 1.16. Even in this favorable case, the expression for ρ often involves algebraic functions which can prove difficult to manipulate symbolically. The purely algebraic approach proposed in Section 2.6 is more suitable for symbolic computation.

2. Algebraic Invariants

In this section we provide a global algebraic counterpart to the local smooth construction presented in Section 1. It can be seen also as a constructive alternative to [**41**].

To a cross-section we associate a graph-section ideal. It is the ideal of the intersection of a generic orbit with the cross-section. As such it is given as an ideal in the polynomial ring over the field of rational functions. We show that the field of definition of the graph-section ideal is actually the field of rational invariants and that the ideal is prime over this field.

The replacement invariants are defined as the zeros of the graph-section ideal. A replacement invariant is a tuple of algebraic invariants in terms of which rational and algebraic invariants can trivially be written. It consequently generates, over $\mathbb{K}$, a field extension of the field of rational invariants. The ideal of the cross-section is the set of relations among the components of a replacement invariant. Accordingly, the field of algebraic invariants is isomorphic to the field of algebraic functions on the cross-section. The invariantization process introduced in this section makes the isomorphism computable with an algorithm that is based on algebraic elimination. In the next section we shall see that the replacement invariants are the analogues of the normalized invariants while the algebraic invariantization provides a computational solution to smooth invariantization.

We shall assume in this section that the base field $\mathbb{K}$ is of characteristic zero and $\bar{\mathbb{K}}$ is its algebraic closure. The definitions we give attempt at being pragmatic from a computational point of view, and ready for use for implementation in a computer algebra system. In order to keep the presentations reasonably self-contained, we included some proofs from [**23**].

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 $\bar{\mathbb{K}}^l$. 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 $\mathcal{Z} = \bar{\mathbb{K}}^n$.

Throughout the section $\lambda = (\lambda_1, \dots, \lambda_l)$ 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 $\mathcal{G} \subset \bar{\mathbb{K}}^l$ and $\mathcal{Z} = \bar{\mathbb{K}}^n$, 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.

In [**41**] a rational action of an algebraic group $\mathcal{G}$ on $\mathcal{Z}$ is a homomorphism from $\mathcal{G}$ to the group of birational automorphisms of $\mathcal{Z}$ such that there is a rational mapping $\mathcal{G} \times \mathcal{Z} \to \mathcal{Z}$ that agrees with it on some dense open subset. On an open dense set of $\mathcal{Z}$ such a homomorphism can be defined by a rational map. Because this latter rational mapping defines the action uniquely, we choose a definition for a rational action that is closer to algebraic computations. Our first condition actually imposes that we consider *good actions*.

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

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

We may assume that the action is defined by rational functions with a common denominator h. Let $H = \{1, h, h^2, \ldots\}$ be the semigroup generated by h, then $H^{-1}\mathbb{K}[\lambda, z]$ denotes the localization of the polynomial ring at H,

$$g(\bar{\lambda}, \bar{z}) = (g_1(\bar{\lambda}, \bar{z}), \ldots, g_n(\bar{\lambda}, \bar{z})) \\ \text{for} \quad g_1, \ldots, g_n \in H^{-1}\mathbb{K}[\lambda_1, \ldots, \lambda_l, z_1, \ldots, z_n]. \tag{4}$$

We make the following additional assumptions about the group action.

Assumption 2.2.

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 dense open set 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 of g.*

2.2. *Rational and Algebraic Invariants*

We base our approach on rational invariants. Algebraic invariants are elements that are algebraic over the field of rational invariants. Such invariants arise in differential geometry, as illustrated in Section 4.

A rational invariant is a rational function $r : \mathcal{Z} \to \mathcal{Z}$ which is constant along an orbit: $r(g(\bar{\lambda}, \bar{z})) = r(\bar{z})$ where defined. We give an equivalent definition that is closer to algebraic computation and following [**11**, Sect. 2.1].

Definition 2.3. A rational function $r \in \mathbb{K}(z)$ is a *rational invariant* if $r(g(\lambda, z)) = r(z) \bmod G$. In other words, if $r = p/q$, with $p, q \in \mathbb{K}[z]$ of degree d or less, r is a rational invariant if

$$h^d(\lambda, z)(q(g(\lambda, z))p(z) - p(g(\lambda, z))q(z)) \in G.$$

Basic results about rational invariants of a rational action are presented in [**41**]. The set of rational invariants forms a field that we denote by $\mathbb{K}(z)^G$. Its transcendence degree over $\mathbb{K}$ is the codimension of the generic orbits of the rational action. The number of generating rational invariants is thus at least the codimension of the generic orbits. Though the emphasis of computational invariant theory has been on polynomial invariants, rational invariants can also be interesting in application as they separate generic orbits [**42**], [**41**].

Definition 2.4. An *algebraic invariant* is an element of the algebraic closure of $\mathbb{K}(z)^G$ that we denote $\overline{\mathbb{K}(z)}^G$.

We choose to write $\overline{\mathbb{K}(z)}^G$ and not $\overline{\mathbb{K}(z)^G}$ for aesthetic reasons, though the latter can be considered as more appropriate.

In Section 2.4 we introduce replacement invariants as specific n-tuples of algebraic invariants. The rewriting of a rational or algebraic invariant in terms of them is a simple replacement of the coordinate functions by the corresponding elements of the tuple. The relationships on the components of a replacement invariants are provided by the equations of the cross-section, defined in the next section. They can thus be chosen with a lot of freedom.

2.3. *Graph of the Action and Cross-Section*

Central in the construction of [**23**], as well as in [**32**], [**9**], [**42**], [**41**], is the ideal

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

where $Z = (Z_1, \ldots, Z_n)$ is a new set of variables and $(Z - g(\lambda, z))$ stands for the ideal $(Z_1 - g_1(\lambda, z), \ldots, Z_n - g_n(\lambda, z))$ that is defined in $H^{-1}\mathbb{K}[\lambda, z, Z]$. The ideal $G + (Z - g(\lambda, z))$ is also considered in $H^{-1}\mathbb{K}[\lambda, z, Z]$. Note that $(G + (Z - g(\lambda, z)) \cap \mathbb{K}[\lambda, z, Z] = G + (hZ_i - hg_i(\lambda, z)) : h^\infty$. The variety of O is the Zariski closure of the *graph of the action*[6]

$$\mathcal{O} = \{(\bar{z}, \bar{z}') \mid \exists\, \bar{\lambda} \in \mathcal{G} \text{ s.t. } \bar{z}' = g(\bar{\lambda}, \bar{z})\} \subset \mathcal{Z} \times \mathcal{Z}.$$

The set $\mathcal{O}$ is the projection of the image of the rational map $\mathcal{G} \times \mathcal{Z} \to \mathcal{G} \times \mathcal{Z} \times \mathcal{Z}$ that associates $(\bar{\lambda}, \bar{z}, g(\bar{\lambda}, \bar{z}))$ to $(\bar{\lambda}, \bar{z})$. As the corresponding elimination ideal, O is the ideal of $\mathcal{O}$.

We mainly use the extension O^e of O in $\mathbb{K}(z)[Z]$. The ideal O^e is unmixed dimensional [**41**, Lemma 2.2]. Its dimension s is the dimension of the generic orbits.

Geometrically speaking, a *cross-section of degree d* is a variety that intersects generic orbits in d simple points. We introduce a definition in terms of ideals as it provides an algebraic way to test if a variety is a cross-section.

Definition 2.5. A prime ideal P in $\mathbb{K}[Z]$ of codimension s defines a *cross-section* to the orbits of the rational action $g : \mathcal{G} \times \mathcal{Z} \to \mathcal{Z}$ if the *graph-section ideal* $I^e = O^e + P$ of $\mathbb{K}(z)[Z]$ is radical and zero dimensional. If d is the dimension of $\mathbb{K}(z)[Z]/I^e$ as a $\mathbb{K}(z)$-vector space, we say that P defines a *cross-section of degree d*.

[6] By the standard definition the graph of a map $\varphi : A \to B$ is a subset of $A \times B$ and, therefore, the graph of the map g belongs to $\mathcal{G} \times \mathcal{Z} \times \mathcal{Z}$. We choose, however, to follow the terminology of [**41**] and use the term the *graph of the action* for the projection of the graph of g to $\mathcal{Z} \times \mathcal{Z}$.

The cross-section is the variety $\mathcal{P}$ of P. It intersects generic orbits transversally in d simple points [**23**, Prop. 3.2]. By the Noether normalization theorem, we can always choose a generic affine space of codimension s as a cross-section [**23**, Theorem 3.3].

Theorem 2.6. *To each point $(a_{ij})_{1\leq i\leq s, 0\leq j\leq n}$ outside an algebraic subset of $\mathbb{K}^{s(n+1)}$ we can associate a linear cross-section to the orbits defined by*

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

Let us note here an algorithmic way to check that P defines a cross-section. Testing transversality beforehand, as explained in Section 1.3, is nonetheless worthwhile. An ideal of $\mathbb{K}(z)[Z]$ is zero dimensional iff its Gröbner basis has an element whose leading term is $Z_i^{d_i}$ for all $1 \leq i \leq n$ [**2**, Theorem 6.54]. Besides, the Seidenberg criterion [**2**] provides a test for a zero-dimensional ideal to be radical. The degree of the cross-section is then the finite number of terms that are not multiples of the leading terms of the elements of the Gröbner basis.

The key observation for our algebraic construction is the following theorem. The part concerning O^e can be considered as a constructive version of [**41**, Lemma 2.4]: there exists a basis of O^e that consists of polynomials in $\mathbb{K}(z)^G[Z]$.

Theorem 2.7. *The reduced Gröbner basis of the graph ideal O^e and the graph-section ideal I^e with respect to any term ordering on Z consists of polynomials in $\mathbb{K}(z)^G[Z]$.*

Proof. We first prove that if $q(z, Z)$ belongs to O, then $q(g(\bar{\lambda}, z), Z)$ belongs to O^e for all $\bar{\lambda} \in \mathcal{G}$. A point $(\bar{z}, \bar{z}') \in \mathcal{O}$ 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 the Hilbert Nullstellensatz the numerator of $q(g(\bar{\lambda}, z), Z)$ belongs to O and therefore $q(g(\bar{\lambda}, z), Z) \in O^e$.

Let $Q = \{q_1, \ldots, q_\kappa\}$ be the reduced Gröbner basis of O^e for a given term order on Z. From what precedes, $q_i(g(\bar{\lambda}, z), Z)$ belongs to O^e. It has the same support[7] 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.

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 Gröbner basis for O^e belong to $\mathbb{K}(z)^G$. 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. □

[7] The support here is the set of terms in Z with nonzero coefficients.

The result was proved in [**23**, Theorems 2.13 and 3.5]. We repeated the proof here so that the paper is self-contained. We furthermore show in [**23**] that the coefficients of a reduced Gröbner basis of I^e, or O^e, form a generating set for $\mathbb{K}(z)^G$. A simple algorithm to rewrite any rational invariants in terms of this generating set is described there as well.

Example 2.8 (Scaling). The multiplicative group, already considered in Example 1.19, is an algebraic group defined by the ideal

$$G = (1 - \lambda_1\lambda_2) \subset \mathbb{K}[\lambda_1, \lambda_2].$$

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 $\bar{\mathbb{K}}^2$. It is given by the following polynomials of $\mathbb{K}[\lambda_1, \lambda_2, z_1, z_2]$,

$$g_1 = \lambda_1 z_1, \qquad g_2 = \lambda_1 z_2.$$

A reduced Gröbner basis of O^e is $\{Z_2 - (z_2/z_1)Z_1\}$ and we can check that z_2/z_1 is a rational invariant (Theorem 2.7).

The ideal $P = (Z_1 - 1)$ defines a section of degree 1: a reduced Gröbner basis of $I^e = O^e + P$ is given by $\{Z_1 - 1, Z_2 - z_2/z_1\}$. We can see that Theorem 2.7 is verified.

The unit circle defined by $P = (Z_1^2 + Z_2^2 - 1)$ is a cross-section of degree 2: a reduced Gröbner basis of $I^e = O^e + P$ is given by $\{Z_1^2 - z_1^2/(z_1^2 + z_2^2), Z_2 - (z_2/z_1)Z_1\}$. Theorem 2.7 is still verified.

Example 2.9 (Rotation). The special orthogonal group, already considered in Example 1.17, is an algebraic group defined by the ideal

$$G = (\lambda_1^2 + \lambda_2^2 - 1) \subset \mathbb{K}[\lambda_1, \lambda_2].$$

The neutral element is $e = (1, 0)$ 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 $\bar{\mathbb{K}}^2$ is given by the following polynomials of $\mathbb{K}[\lambda_1, \lambda_2, z_1, z_2]$:

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

A reduced Gröbner basis of O^e is $Q = \{Z_1^2 + Z_2^2 - (z_1^2 + z_2^2)\}$. The ideal $P = (Z_2)$ defines a cross-section of degree 2: the reduced Gröbner basis of I^e w.r.t. any term order is $\{Z_2, Z_1^2 - (z_1^2 + z_2^2)\}$. Theorem 2.7 is verified.

Example 2.10 (Translation + reflection). We consider the algebraic group $\mathbb{K} \times \{-1, 1\}$. It is defined by

$$G = (\lambda_2^2 - 1) \subset \mathbb{K}[\lambda_1, \lambda_2].$$

This group has two components: $G = (\lambda_2 - 1) \cap (\lambda_2 + 1)$. 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 the action of $\mathcal{G}$ on $\bar{\mathbb{K}}^2$ as translation parallel to the first coordinate axis and reflection w.r.t. this axis. It is defined by the following polynomials of $\mathbb{K}[\lambda_1, \lambda_2, z_1, z_2]$:

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

A reduced Gröbner basis of O^e is $Q = \{Z_2^2 - z_2^2\}$. The ideal $P = (Z_1 - Z_2)$ defines a cross-section of degree 2: A reduced Gröbner basis of I^e is given by $\{Z_1 - Z_2, Z_2^2 - z_2^2\}$.

This example is to be compared with Example 1.20. In contrast with the local construction illustrated there, we produce here rational functions that are invariant with respect to the entire group.

2.4. *Replacement Invariants*

Given a cross-section $\mathcal{P}$ of degree d we introduce d distinct n-tuples of elements that are algebraic over the field of rational invariants. Each n-tuple has an important *replacement* property: any rational invariant can be rewritten in terms of its components by a simple substitution of the variables by the corresponding elements from the tuple.

A reduced Gröbner basis Q of $I^e = O^e + P$ is contained in $\mathbb{K}(z)^G[Z]$ (Theorem 2.7) 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 distinct zeros whose components belong to $\overline{\mathbb{K}(z)}^G$ [**11**, Prop. 2.15]. We call such a zero 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 2.11. 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 $\xi = (\xi_1, \ldots, \xi_n)$ of algebraic invariants that forms a zero of I^e.

Thus d replacement invariants $\xi^{(1)}, \ldots, \xi^{(d)}$ are associated to a cross-section of degree d. The name is owed to the next theorem which can be compared with the Thomas replacement theorem discussed in [**12**, p. 38] and revisited in this paper as Theorem 1.9.

Theorem 2.12. *Let $\xi = (\xi_1, \ldots, \xi_n)$ be a replacement invariant. If $r \in \mathbb{K}(z)^G$ then $r(z_1, \ldots, z_n) = r(\xi_1, \ldots, \xi_n)$ in $\overline{\mathbb{K}(z)}^G$.*

Proof. Write $r = p/q$ with p, q relatively prime. By [**23**, Lemma 2.14], $p(z)q(Z) - q(z)p(Z) \in O^e \subset I^e$ and, therefore, $p(Z) - (p(z)/q(z))q(Z) = p(Z) - r(z)q(Z) \in I^e$. Since ξ is a zero of I^e, we have $p(\xi) - r(z)q(\xi) = 0$. By [**23**, Lemma 3.6] $p(Z), q(Z)$ cannot belong to P and therefore cannot be zero divisors modulo I^e. Thus $q(\xi) \neq 0$ and the conclusion follows. □

When the cross-section is of degree 1, there is a unique replacement invariant. The dimension of $\mathbb{K}(z)[Z]/I^e$ as a $\mathbb{K}(z)$ vector space is 1 so that, independently of the chosen term order, the reduced Gröbner basis of I^e is given then by $\{Z_i - r_i(z) \mid 1 \leq i \leq n\}$, where the $r_i \in \mathbb{K}(z)^G$ according to Theorem 2.7. The unique replacement invariant is thus $(r_1, \ldots, r_n)$. Theorem 2.12 implies then that $\mathbb{K}(z)^G = \mathbb{K}(r_1, \ldots, r_n)$. A generalization of this fact appears in [**23**, Theorem 3.6]: $\mathbb{K}(z)^G$ is generated by the coefficients of the Gröbner basis of O^e or I^e.

Example 2.13 (Scaling). Consider the group action from Example 2.8. The cross-section defined there by $P = (Z_1 - 1)$ is of degree 1. Since $I^e = (Z_1 - 1, Z_2 - z_2/z_1)$, the unique replacement invariant associated to $\mathcal{P}$ is $\xi = (1, z_2/z_1)$ and, therefore, $\mathbb{K}(z)^G = \mathbb{K}(z_2/z_1)$.

Example 2.14 (Rotation). Consider the group action from Example 2.9. The cross-section defined there by $P = (Z_2)$ is of degree 2. 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 algebraic over $\mathbb{K}(z)^G$ and defined by $\rho^2 = (z_1^2 + z_2^2)$.

Example 2.15 (Translation + reflection). Consider the group action from Example 2.10. The cross-section defined there by $P = (Z_1 - Z_2)$ 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.

As an introduction to the next section, note that $I^e = (Z_1 - z_2, Z_2 - z_2) \cap (Z_1 + z_2, Z_2 + z_2)$ is a reducible ideal of $\mathbb{K}(z)[Z]$, while $I^G = I^e \cap \mathbb{K}(z)^G[Z]$ is a prime ideal of $\mathbb{K}(z)^G[Z]$.

2.5. *Algebraic Invariants as Functions on the Cross-Section*

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 use the replacement invariants to show that $\mathbb{K}(\mathcal{P})$ is an algebraic extension of degree d of the field of rational invariants $\mathbb{K}(z)^G$.

The field $\mathbb{K}(\xi)$, for any replacement invariant ξ, is an algebraic extension of $\mathbb{K}(z)^G$. Indeed, $\mathbb{K}(z)^G \subset \mathbb{K}(\xi)$ and ξ is algebraic over $\mathbb{K}(z)^G$. This leads to the following results.

Lemma 2.16. *$I^G = I^e \cap \mathbb{K}(z)^G[Z]$ is a prime ideal of $\mathbb{K}(z)^G[Z]$.*

Proof. Let $I^{(1)}$ and $I^{(2)}$ be prime divisors of I^G in $\mathbb{K}(z)^G[Z]$ and consider replacement invariants $\xi^{(1)}$ and $\xi^{(2)}$ that are $\overline{\mathbb{K}(z)}^G$-zeros of $I^{(1)}$ and $I^{(2)}$, respectively. Due to Theorem 2.12, $\mathbb{K}(\xi^{(i)}) = \mathbb{K}(z)^G(\xi^{(i)})$. There is therefore a $\mathbb{K}(z)^G$-isomorphism $\mathbb{K}(z)^G[Z]/I^{(i)} \cong \mathbb{K}(\xi^{(i)})$ for $i = 1$ or 2. On the other hand, we have

$\mathbb{K}(\xi^{(i)}) \cong \mathbb{K}(\mathcal{P})$ since P is the ideal of all relationships on the components of $\xi^{(i)}$ over $\mathbb{K}$ [**23**, Prop. 3.4]. Thus

$$\mathbb{K}(z)^G[Z]/I^{(1)} \cong \mathbb{K}(\xi^{(1)}) \cong \mathbb{K}(\mathcal{P}) \cong \mathbb{K}(\xi^{(2)}) \cong \mathbb{K}(z)^G[Z]/I^{(2)}.$$

We have an isomorphism between $\mathbb{K}(z)^G[Z]/I^{(1)}$ and $\mathbb{K}(z)^G[Z]/I^{(2)}$ that leaves $\mathbb{K}(z)^G$ fixed and maps the class of Z modulo $I^{(1)}$ to the class of Z modulo $I^{(2)}$. Therefore $I^{(1)} = I^{(2)}$ so that I^G is prime. □

Theorem 2.17. *The field $\mathbb{K}(\mathcal{P})$ is an algebraic extension of $\mathbb{K}(z)^G$ of degree d, the degree of the cross-section $\mathcal{P}$.*

Proof. For any replacement invariant ξ we have $\mathbb{K}(z)^G[Z]/I^G \cong \mathbb{K}(\xi) \cong \mathbb{K}(\mathcal{P})$. Since the dimension of $\mathbb{K}(z)^G[Z]/I^G$ as a $\mathbb{K}(z)^G$-vector space is d, the field $\mathbb{K}(\mathcal{P})$ is an algebraic extension of $\mathbb{K}(z)^G$ of degree d. □

In particular, if $\mathcal{P}$ is a cross-section of degree 1 we have $\mathbb{K}(\mathcal{P}) \cong \mathbb{K}(z)^G$. In all cases we have the isomorphism $\overline{\mathbb{K}(\mathcal{P})} \cong \overline{\mathbb{K}(z)}^G$ obtained in [**41**, Sect. 2.5] by different means.

2.6. *Algebraic Invariantization*

In this section we introduce invariantization as a projection from the ring of univariate polynomials over $\mathbb{K}[z]$ to the ring of univariate polynomials over $\mathbb{K}(z)^G$. It depends on the choice of a cross-section and is computable by algebraic elimination. As this projection extends to univariate polynomials over $\mathbb{K}(\mathcal{P})$ it can be understood as the computable counterpart to the isomorphism $\overline{\mathbb{K}(\mathcal{P})} \cong \overline{\mathbb{K}(z)}^G$ that follows from Theorem 2.17.

The ideal of the cross-section $\mathcal{P}$ is taken alternatively in $\mathbb{K}[z]$ and in $\mathbb{K}[Z]$. To avoid confusion we shall use in this section P_z and P_Z to distinguish the two cases. The localization of $\mathbb{K}[z]$ at P_z is denoted by $\mathbb{K}[z]_{\mathcal{P}}$. By [**23**, Lemma 3.6], $\mathbb{K}(z)^G \subset \mathbb{K}[z]_{\mathcal{P}}$.

The first approach to algebraic invariantization that [**12**] suggests is to consider a replacement invariant ξ associated to $\mathcal{P}$ and the following chain of homomorphisms:

$$\begin{array}{ccccc} \mathbb{K}[z]_{\mathcal{P}} & \xrightarrow{\pi} & \mathbb{K}(\mathcal{P}) & \xrightarrow{\varphi_\xi} & \overline{\mathbb{K}(z)}^G, \\ r(z) & \longmapsto & r(z)+P_z & \longmapsto & r(\xi). \end{array} \tag{5}$$

The restriction of $\iota_\xi = \varphi_\xi \circ \pi : \mathbb{K}[z]_{\mathcal{P}} \to \overline{\mathbb{K}(z)}^G$ to $\mathbb{K}(z)^G$ is the identity map by Theorem 2.12. We call the image of a rational function $r(z) \in \mathbb{K}[z]_{\mathcal{P}}$ under ι_ξ its *ξ-invariantization*.

If $\mathcal{P}$ is a cross-section of degree d there are d distinct associated replacement invariants $\xi^{(1)}, \ldots, \xi^{(d)}$. The image $\iota_\xi(r(z)) = r(\xi)$ depends on the chosen replacement invariant ξ. This is not the case of the minimal polynomial of $r(\xi)$ over $\mathbb{K}(z)^G$ which depends only on $\mathcal{P}$, as we shall see below. We therefore define the $\mathcal{P}$-invariantization as a map taking a univariate polynomial over $\mathbb{K}[z]_\mathcal{P}$ to a univariate polynomial over $\mathbb{K}(z)^G$. This second approach corresponds to the definition of smooth invariantization given in Section 1.4, as is detailed in Section 3.

Definition 2.18. The $\mathcal{P}$-invariantization $\iota\alpha$ of a monic univariate polynomial $\alpha \in \mathbb{K}[z]_\mathcal{P}[\zeta]$ is the squarefree part of $\prod_{i=1}^{d} \alpha(\xi^{(i)}, \zeta)$, where $\xi^{(1)}, \ldots, \xi^{(d)}$ are the d replacement invariants associated to the cross-section $\mathcal{P}$.

Readers familiar with computer algebra techniques can see that $\iota\alpha$ belongs to $\mathbb{K}(z)^G[\zeta]$ with the following line of argument. The replacement invariants $\xi^{(1)}, \ldots, \xi^{(d)}$ are the d distinct zeros of the zero-dimensional prime ideal I^G of $\mathbb{K}(z)^G[Z]$. By a transcription of the primitive element theorem, see, for instance, [**19**, Prop. 4.2.2(3)], they are thus the images by a polynomial map $\psi : \theta \mapsto (\psi_1(\theta), \ldots, \psi_n(\theta))$ over $\mathbb{K}(z)^G$ of the roots $\theta^{(1)}, \ldots, \theta^{(d)} \in \overline{\mathbb{K}(z)}^G$ of an irreducible univariate polynomial of degree d with coefficients in $\mathbb{K}(z)^G$. The coefficients of the polynomial

$$\prod_{i=1}^{d} \alpha(\xi^{(i)}, \zeta) = \prod_{i=1}^{d} \alpha(\psi(\theta^{(i)}), \zeta)$$

are elements of the field extension $\mathbb{K}(z)^G(\theta^{(1)}, \ldots, \theta^{(d)})$ of $\mathbb{K}(z)^G$ that are invariant under all permutations of the $\theta^{(i)}$. By [**47**, Sect. 8.1] or [**15**, Theorem 8.15], that polynomial belongs to $\mathbb{K}(z)^G[\zeta]$ and thus so does its squarefree part $\iota\alpha$ [**47**, Sect. 8.1].

For a Galois theory-oriented reader the direct proof is provided below. By definition $\iota\alpha$ belongs to the extension $\mathbb{K}(\xi^{(1)}, \ldots, \xi^{(d)})$, which we denote by $\mathbb{K}_\xi$. Due to Theorem 2.12, $\mathbb{K}_\xi = \mathbb{K}(z)^G(\xi^{(1)}, \ldots, \xi^{(d)})$. In order to prove that $\iota\alpha \in \mathbb{K}(z)^G[\zeta]$, we will show that this polynomial is preserved by the Galois group of the extension $\mathbb{K}_\xi \supset \mathbb{K}(z)^G$. We need the following proposition.

Proposition 2.19. *Let $\{\xi^{(1)}, \ldots, \xi^{(d)}\}$ be the set of replacement invariants corresponding to the cross-section $\mathcal{P}$ of degree d. Then the field $\mathbb{K}_\xi = \mathbb{K}(\xi^{(1)}, \ldots, \xi^{(d)})$ is a splitting field of a univariate polynomial $\beta(z, \zeta) \in \mathbb{K}(z)^G[\zeta]$ of degree d. The Galois group of the extension $\mathbb{K}_\xi \supset \mathbb{K}(z)^G$ permutes the n-tuples $\xi^{(1)}, \ldots, \xi^{(d)}$.*

Proof. Due to the replacement Theorem 2.12 one has the equality $\mathbb{K}(\xi^{(1)}) = \mathbb{K}(z)^G(\xi^{(1)})$. From Corollary 2.17 it follows that $\mathbb{K}(z)^G(\xi^{(1)})$ is an extension of degree d of $\mathbb{K}(z)^G$ for $i = 1..d$. Since $\mathbb{K}$ is assumed to be of characteristic zero, the components $\xi_1^{(1)}, \ldots, \xi_n^{(1)}$ of n-tuple $\xi^{(1)}$ are separable over $\mathbb{K}(z)^G$. Hence there exists a primitive element $\theta_1 \in \mathbb{K}(\xi^{(1)})$, such that $\mathbb{K}(\xi^{(1)}) = \mathbb{K}(z)^G(\xi^{(1)}) =$

$\mathbb{K}(z)^G(\theta_1)$, where θ_1 is a root of an irreducible univariate polynomial $\beta(z,\zeta) \in \mathbb{K}(z)^G[\zeta]$ of degree d [**7**, Theorem 5.4.1].

Let $\sigma_{ji} : \mathbb{K}(\xi^{(i)}) \to \mathbb{K}(\xi^{(j)})$ be the $\mathbb{K}(z)^G$-isomorphism induced by exchanging $\xi^{(i)}$ and $\xi^{(j)}$. Then $\theta_j = \sigma_{j1}(\theta_1)$ is a primitive element of the extension $\mathbb{K}(\xi^{(j)}) \supset \mathbb{K}(z)^G$. Indeed, since θ_1 is the primitive element of $\mathbb{K}(z)^G(\xi^{(1)})$ for each $i = 1..n$, there exists a polynomial ψ_i over $\mathbb{K}(z)^G$ such that $\xi_i^{(1)} = \psi_i(\theta_1)$. Since σ_{j1} is a $\mathbb{K}(z)^G$-isomorphism, it follows that $\xi_i^{(j)} = \sigma_{j1}(\xi_i^{(1)}) = \sigma_{j1}(\psi_i(\theta_1)) = \psi_i(\sigma_{j1}(\theta_1)) = \psi_i(\theta_j)$ for $i = 1..n$. Thus θ_j is a primitive element of $\mathbb{K}(\xi^{(j)}) \supset \mathbb{K}(z)^G$, and so $\mathbb{K}_\xi = \mathbb{K}(z)^G(\theta_1, \ldots, \theta_d)$.

In addition, we proved that n-tuples $\xi^{(1)}, \ldots, \xi^{(d)}$ are images of $\theta_1, \ldots, \theta_d$ under the polynomial map $\psi = (\psi_1, \ldots, \psi_n) : \overline{\mathbb{K}(z)}^G \to [\overline{\mathbb{K}(z)}^G]^n$, where the coefficients of the univariate polynomials $\psi_1, \ldots, \psi_n$ are in $\mathbb{K}(z)^G$. Since $\xi^{(1)}, \ldots, \xi^{(d)}$ are distinct tuples, then $\theta_1, \ldots, \theta_d$ are distinct elements of $\overline{\mathbb{K}(z)}^G$. We will now show that $\theta_1, \ldots, \theta_d$ are roots of the minimal polynomial $\beta \in \mathbb{K}(z)^G[\zeta]$ that defines θ_1.

Indeed, since the field $\mathbb{K}(z)^G$ is fixed under σ_{j1} for $j = 1..d$, then so is the polynomial β. Thus $\theta_j = \sigma_{j1}(\theta_1)$ are roots of the polynomial β. It follows that $\mathbb{K}_\xi = \mathbb{K}(z)^G(\theta_1, \ldots, \theta_d)$ is the splitting field of an irreducible univariate polynomial $\beta \in \mathbb{K}(z)^G[\zeta]$ of degree d.

The elements of the $\mathrm{Gal}(\mathbb{K}_\xi/\mathbb{K}(z)^G)$ permute the roots $\theta_1, \ldots, \theta_d$ of the polynomial β and, therefore, it permutes the tuples $\xi^{(j)} = \psi(\theta_j)$ for all $j = 1..d$. □

Corollary 2.20. *Let $\alpha(z,\zeta) \in \mathbb{K}[z]_{\mathcal{P}}$ be a univariate polynomial over $\mathbb{K}[z]_{\mathcal{P}}$. Then its $\mathcal{P}$-invariantization $\iota\alpha$ is a polynomial over $\mathbb{K}(z)^G$.*

Proof. The Galois group of the extension $\mathbb{K}_\xi \supset \mathbb{K}(z)^G$ induces permutations of the n-tuples $\xi^{(1)}, \ldots, \xi^{(d)}$. Thus the polynomial $p(\zeta) = \prod_{i=1}^d \alpha(\xi^{(i)}, \zeta) \in \mathbb{K}_\xi[\zeta]$ is fixed under $\mathrm{Gal}(\mathbb{K}_\xi/\mathbb{K}(z)^G)$. Hence its coefficients belong to $\mathbb{K}(z)^G$. By definition $\iota\alpha$ is the square-free part of $p(\zeta)$ and, hence, it is also fixed under the Galois group, since it has the same roots in $\mathbb{K}_\xi$ as $p(\zeta)$ itself [**7**, Prop. 5.3.8], and the Galois group permutes these roots. Thus its coefficients of $\iota\alpha$ are in $\mathbb{K}(z)^G$. □

The following properties follow directly from the definition of the map ι:

1. A $\overline{\mathbb{K}(z)}^G$-zero of $\iota\beta$ is a $\overline{\mathbb{K}(z)}^G$-zero of a $\beta(\xi^{(i)}, \zeta)$ and conversely.
2. If $\beta \in \mathbb{K}(z)^G[\zeta]$, then $\iota\beta = \beta$ since $\beta(\xi^{(i)}, \zeta) = \beta(z, \zeta)$ by Theorem 2.12.
3. If $\alpha \equiv \beta \bmod P_z$, then $\iota\alpha = \iota\beta$ since the elements of P_z vanish on all $\xi^{(i)}$.

The last property shows that ι induces a map φ from the set of monic polynomials of $\mathbb{K}(\mathcal{P})[\zeta]$ to the set of monic polynomials of $\mathbb{K}(z)^G[\zeta]$ s.t. $\iota = \varphi \circ \pi$.

From the first property it follows that $\beta(\xi^{(i)}, \zeta)$ divides $\iota\beta(z,\zeta)$ in $\mathbb{K}(\xi^{(i)})[\zeta] \supset \mathbb{K}(z)^G[\zeta]$ when $\beta(\xi^{(i)}, \zeta)$ is squarefree. Since $\mathbb{K}(\mathcal{P}) \cong \mathbb{K}(\xi^{(i)})$ this amounts to the following proposition that will be used in Section 3.3.

Proposition 2.21. *Let β be a monic polynomial of $\mathbb{K}[z]_{\mathcal{P}}[\zeta]$. If β is squarefree when considered in $\mathbb{K}(\mathcal{P})[\zeta]$, then it divides $\iota\beta(z,\zeta)$ in $\mathbb{K}(\mathcal{P})[\zeta]$, i.e., there exists $q(z,\zeta) \in \mathbb{K}[z]_{\mathcal{P}}[\zeta]$ s.t. $\iota\beta(z,\zeta) \equiv q(z,\zeta)\beta(z,\zeta) \bmod P_z$.*

Also we recognize in the definition of the invariantization map the norm of a polynomial in an algebraic extension [**15**, Sect. 8.8]. We reformulate the results extending those of that text, namely:

- $\iota\beta$ can be computed by algebraic elimination.
- if $\beta(\xi^{(i)},\zeta)$ is the minimal polynomial over $\mathbb{K}(\xi^{(i)}) \subset \overline{\mathbb{K}(z)}^G$ of an element in $\overline{\mathbb{K}(z)}^G$, then $\iota\beta$ is the minimal polynomial of this element over $\mathbb{K}(z)^G$.

The algebraic elimination to compute $\iota\beta$ can be performed by several techniques. For a strict generalization of [**15**, Sect. 8.8] one could introduce a resultant formula, as developed in [**8**]. We propose here a formulation in terms of elimination ideals.

Proposition 2.22. *Consider a monic polynomial β in $\mathbb{K}[z]_{\mathcal{P}}[\zeta]$. Its $\mathcal{P}$-invariantization $\iota\beta$ is the squarefree part of the monic generator of $(I^G+\alpha(Z,\zeta))\cap\mathbb{K}(z)^G[\zeta]$ where $\alpha(z,\zeta) \in \mathbb{K}[z][\zeta]$ is the numerator of β.*

Proof. The leading coefficient of $\alpha(Z,\zeta) \in \mathbb{K}[Z][\zeta]$ does not belong to P_Z and, therefore, it does not belong to I^G. It follows that $(I^G+\alpha(Z,\zeta))\cap\mathbb{K}(z)^G[\zeta] \neq (0)$ since I^G is zero dimensional.

Let $\gamma(z,\zeta)$ be the monic generator of $(I^G+\alpha(Z,\zeta))\cap\mathbb{K}(z)^G[\zeta]$. We first prove that $\iota\beta$ divides the squarefree part of $\gamma(z,\zeta)$. The fact that $\gamma(z,\zeta)$ belongs to $I^G+\alpha(Z,\zeta)$ can be written as $\gamma(z,\zeta) \equiv q(z,Z,\zeta)\alpha(Z,\zeta) \bmod I^G$ where $q(z,Z,\zeta) \in \mathbb{K}(z)^G[Z,\zeta]$. Substituting $\xi^{(i)}$ for Z we have $\gamma(z,\zeta) = q'(z,\xi^{(i)},\zeta)\beta(\xi^{(i)},\zeta)$ where $q(z,\xi^{(i)},\zeta)$ and $q'(z,\xi^{(i)},\zeta)$ differ by the factor in $\mathbb{K}[\xi^{(i)}]$ that distinguishes $\alpha(\xi^{(i)},\zeta)$ from $\beta(\xi^{(i)},\zeta)$. Therefore all the factors $\beta(\xi^{(i)},\zeta)$ of $\iota\beta$ divide $\gamma(z,\zeta)$. Since $\iota\beta$ is the squarefree product of $\beta(\xi^{(i)},\zeta)$ it divides the squarefree part of $\gamma(z,\zeta)$.

Conversely, we prove that the squarefree part of $\gamma(z,\zeta)$ divides $\iota\beta$. The $\overline{\mathbb{K}(z)}^G$-zeros of $\alpha(Z,\zeta)+I^G$ are the $(n+1)$-tuples $(\xi^{(i)}, f_{i,j})$, where $f_{i,j}$, $1 \leq j \leq \deg\beta$, are the roots of $\beta(\xi^{(i)},\zeta)$. Since $\gamma(z,\zeta)$ belongs to $\alpha(Z,\zeta)+I^G$ its set of $\overline{\mathbb{K}(z)}^G$-roots includes all the $f_{i,j}$. Thus γ and $\iota\beta$ have the same set of roots. Therefore the squarefree part of γ divides $\iota\beta$. □

Note that the monic generator of $(I^G+\alpha(Z,\zeta))\cap\mathbb{K}(z)^G[\zeta]$ is the monic generator of $(I^e+\alpha(Z,\zeta))\cap\mathbb{K}(z)[\zeta]$. Indeed, this latter is an element of the reduced Gröbner basis of $(\alpha(Z,\zeta)+I^e)$ w.r.t. a term order that eliminates Z. It follows from Proposition 2.7 that it belongs to $\mathbb{K}(z)^G[\zeta]$. Therefore computations over $\mathbb{K}(z)$ lead to the correct result over $\mathbb{K}(z)^G$.

The last proposition provides the computable counterpart of the isomorphism $\overline{\mathbb{K}(\mathcal{P})} \cong \overline{\mathbb{K}(z)}^G$, elements of $\overline{\mathbb{K}(\mathcal{P})}$ or $\overline{\mathbb{K}(z)}^G$ being represented by irreducible monic polynomials over $\mathbb{K}(\mathcal{P})$ or $\mathbb{K}(z)^G$, respectively.

Proposition 2.23. *Let α be a monic polynomial of $\mathbb{K}[z]_{\mathcal{P}}[\zeta]$. The polynomial $\iota\alpha \in \mathbb{K}(z)^G[\zeta]$ is irreducible if and only if α is a power of an irreducible polynomial when considered in $\mathbb{K}(\mathcal{P})[\zeta]$.*

Proof. Note that $\iota(\beta\,\gamma)$, for $\beta, \gamma \in \mathbb{K}[z]_{\mathcal{P}}[\zeta]$, is the squarefree part of the product $\iota\beta\,\iota\gamma$. So if α considered in $\mathbb{K}(\mathcal{P})[\zeta]$ is the product of two relatively prime factors, then $\iota\alpha$ cannot be irreducible.

We can replace α by its squarefree part when considered in $\mathbb{K}(\mathcal{P})[\zeta]$ without loss of generality and thus assume for the converse implication that $\alpha(z, \zeta)$ is irreducible there. Let $\bar{\alpha} \in \mathbb{K}[z][\zeta]$ be obtained from α by cleaning up the denominators. Then $\bar{\alpha}(Z, \zeta)$ is irreducible modulo I^G so that $(\bar{\alpha}(Z, \zeta) + I^G)$ is prime. The monic generator $\iota\alpha$ of $(\alpha(Z, \zeta) + I^G) \cap \mathbb{K}(z)[\zeta]$ is thus irreducible. □

The following example illustrates various properties of the $\mathcal{P}$-invariantization map ι.

Example 2.24 (Scaling). We return to the scaling action of Example 2.8 with the unit circle as cross-section of degree 2. For $P_Z = (Z_1^2 + Z_2^2 - 1)$ we have $I^e = (Z_1^2 - z_1^2/(z_1^2 + z_2^2), Z_2 - (z_2/z_1)Z_1)$ so that the two replacement invariants are

$$\xi^{(\pm)} = \left(\frac{\pm z_1}{\sqrt{z_1^2 + z_2^2}}, \frac{\pm z_2}{\sqrt{z_1^2 + z_2^2}} \right).$$

The invariantization of $\alpha = \zeta - z_1$ is $\iota\alpha = \zeta^2 - z_1^2/(z_1^2 + z_2^2)$. We have $\iota\alpha = (\zeta + z_1)\alpha + [z_1^2/(z_1^2 + z_2^2)](z_1^2 + z_2^2 - 1) \equiv (\zeta + z_1)\alpha \bmod P_z$. We obtained $\iota\alpha$ by computing the reduced Gröbner basis of the ideal $(\zeta - Z_1, Z_1^2 - z_1^2/(z_1^2 + z_2^2), Z_2 - (z_2/z_1)Z_1)$ with a term order that eliminates Z_1 and Z_2. Note that, although α defines a polynomial function, its invariantization defines two algebraic invariants $\pm z_1/\sqrt{z_1^2 + z_2^2}$.

The invariantization of $\beta = \zeta^3 + \zeta^2 + z_2\zeta + 1$ is $\iota\beta = \zeta^6 + 2\,\zeta^5 + \zeta^4 + 2\,\zeta^3 + [(z_2^2 + 2z_1^2)/(z_1^2 + z_2^2)]\,\zeta^2 + 1$. We have $\iota\beta \equiv (\zeta^3 + \zeta^2 - z_2\zeta + 1)\beta \bmod P_z$.

In the next two instances the monic polynomial is equal modulo P_z to a polynomial in $\overline{\mathbb{K}(z)}^G[\zeta]$. As a consequence, the invariantization equals the original polynomial modulo P_z.

The polynomial $\gamma = \zeta - z_1^2$ is equal to its $\mathcal{P}$-invariantization $\iota\gamma = \zeta - z_1^2/(z_1^2 + z_2^2) \equiv \gamma \bmod P_z$.

The irreducible polynomial $\delta = \zeta^2 - [(z_1^2 + z_2^2 - 1)/z_2^2]\zeta - z_1^2/z_2^2$ becomes a reducible modulo P_z: $\delta \equiv \zeta^2 - z_1^2/z_2^2 \bmod P_z$. Its invariantization is thus reducible: $\iota\delta = (\zeta - z_1/z_2)(\zeta + z_1/z_2) \equiv \delta \bmod P_z$.

3. Algebraic Approach to Smooth Constructions

We establish a connection between the smooth and the algebraic constructions. We show that the normalized invariants (Section 1.5) can be viewed as smooth representatives of the replacement invariants (Section 2.4), and that algebraic invariantization (Section 2.6) provides a constructive approach to smooth invariantization (Section 1.3). We start nonetheless by providing an algebraic formulation of a moving frame map of Section 1.6 so as to point out the computational advantages of our new algebraic approach.

To be at the intersection of the hypotheses of the smooth and the algebraic settings we consider a real algebraic group, that is, the set of real points of an algebraic group defined[8] over $\mathbb{R}$. It is a real Lie group [**45**, Chap. 3, Sect. 2.1.2]. Lie groups appearing in applications often satisfy this property.

The local action is given by a rational map that satisfies Asumption 2.2. This guarantees semiregularity of the action on an open set $\mathcal{Z}$ of $\mathbb{R}^n$ as the orbits of nonmaximal dimension are contained in an algebraic set defined by minors of the matrix V of (1), in Section 1.3.

It follows from Theorem 1.6 that, through every point of $\mathcal{Z}$, there exist local cross-sections defined by linear equations over $\mathbb{R}$. Conversely, let P be an ideal defined over $\mathbb{R}$ that defines a cross-section (Definition 2.5) and whose real and complex varieties have the same dimension. Then, for any point $\bar{z} \in \mathcal{Z} \cap \mathcal{P}$ where the matrix (1) is of maximal rank, there is a neighborhood $\mathcal{U}$ on which $\mathcal{P}$ defines a local cross-section, and such points are dense in $\mathcal{P}$.

3.1. *The Moving Frame Map and Ideal*

In Section 1.6 we discussed how the condition $\rho(\bar{z}) \cdot \bar{z} \in \mathcal{P}$ leads to the moving frame map $\rho : \mathcal{Z} \to \mathcal{G}$ that underlies the Fels–Olver construction. In this section we define a moving frame ideal, which is an algebraic counterpart of the moving frame map, and explain the advantage of an approach based on cross-sections.

In the algebraic setting the condition $\rho(\bar{z}) \cdot \bar{z} \in \mathcal{P}$ is described by the ideal $M = (Z - g(\lambda, z) + G + P_Z) \cap \mathbb{K}[z, \lambda]$. Indeed, if $(\bar{z}, \bar{\lambda})$ is a zero of M, in an appropriate open set of $\mathcal{Z} \times \mathcal{G}$, then $\bar{\lambda} \cdot \bar{z} \in \mathcal{P}$. The action is locally free if and only if the extension $M^e \in \mathbb{R}(z)[\lambda]$ is zero dimensional. In this case, the smooth zero $F : \mathcal{U} \to \mathcal{G}$ of M^e, that is, the identity of the group when restricted to $\mathcal{P}$, provides a moving frame map ρ on $\mathcal{U}$.

[8] This implicitly means that we know the ideal G (Section 2.1) from a set of generators with coefficients in $\mathbb{R}$.

Example 3.1 (Scaling). We return to the action of the multiplicative group $\mathbb{R}^*$ of Example 1.19. The multiplicative group $\mathbb{R}^*$ corresponds to the algebraic group $\mathcal{G} \subset \mathbb{R}^2$ defined by the ideal $G = (\lambda_1\lambda_2 - 1)$, which insures that $\lambda_1 \neq 0$. The corresponding algebraic action is described by the ideal $J = (Z_1 - \lambda_1 z_1, Z_2 - \lambda_1 z_2, \lambda_1\lambda_2 - 1)$.

In Example 2.8 we first chose an algebraic cross-section of degree 1 defined by the ideal $P_Z = (Z_1 - 1)$. The unique zero of the corresponding moving frame ideal $M^e = (\lambda_1 - 1/z_1, \lambda_2 - z_1)$ defines the moving frame map $\rho(z_1, z_2) = (1/z_1, z_1) : \mathcal{Z} \to \mathcal{G}$. Note that on $\mathcal{P}$ the map ρ produces the identity of the group $(1, 1)$. The map ρ can be used to invariantize any function as described in Section 1.4. If $f(z)$ is a locally smooth function on $\mathcal{Z}$, then $\bar{\iota} f(z) = f(g(\rho(z), z))$. For instance, the invariantization of the coordinate functions (z_1, z_2) produces normalized invariants $((1/z_1)z_1, (1/z_1)z_2) = (1, z_1/z_2)$.

In Example 2.8 we also considered a circular cross-section of degree 2 defined by the ideal $P_Z = (Z_1^2 + Z_2^2 - 1)$. The corresponding moving frame ideal $M^e = (\lambda_1 - [1/(z_1^2 + z_2^2)]\lambda_2, \lambda_2^2 - (z_1^2 + z_2^2))$ has two zeros $\rho^{\pm}(z_1, z_2) = (\pm 1/\sqrt{z_1^2 + z_2^2}, \pm\sqrt{z_1^2 + z_2^2})$. The condition that ρ produces identity of the group at the points of $\mathcal{P}$ leads to the choice: $\rho(z_1, z_2) = (1/(z_1^2 + z_2^2), \sqrt{z_1^2 + z_2^2})$. The invariantization of the coordinate functions $g(\rho(z_1, z_2), z_1, z_2)$ produces normalized invariants $(z_1/\sqrt{z_1^2 + z_2^2}, z_2/\sqrt{z_1^2 + z_2^2})$.

Example 3.2 (Rotation). We return to the $SO(2)$-action considered in Example 1.17. This action is free on $\mathbb{R}^2 \backslash \{(0, 0)\}$.

In Example 2.14 we defined the corresponding algebraic action by the ideal $J = (Z_1 - \lambda_1 z_1 + \lambda_2 z_2, Z_2 - \lambda_2 z_1 - \lambda_1 z_2, \lambda_1^2 + \lambda_2^2 - 1)$ and chose the algebraic cross-section $\mathcal{P}$ defined by $Z_1 = 0$. The corresponding moving frame ideal

$$M^e = \left(\lambda_1 - \frac{z_2}{z_1}\lambda_2, \lambda_2^2 - \frac{z_1^2}{(z_1^2 + z_2^2)}\right)$$

has two zeros so that the moving frame map is

$$\rho^{\pm}(z_1, z_2) = \left(\pm\frac{z_2}{\sqrt{z_1^2 + z_2^2}}, \pm\frac{z_1}{\sqrt{z_1^2 + z_2^2}}\right).$$

The cross-section $\mathcal{P}$ defines a local cross-section on two open subsets:

$$\mathcal{U}^{(+)} = \mathbb{R}^2 \backslash \{(0, z_2) \mid z_2 \leq 0\} \qquad \text{and} \qquad \mathcal{U}^{(-)} = \mathbb{R}^2 \backslash \{(0, z_2) \mid z_2 \geq 0\}.$$

Since $\rho^{(+)}|_{\mathcal{P}\cap\mathcal{U}^{(+)}} = (1, 0)$ is the identity of the group, the moving frame map $\rho = \rho^{(+)}$ on $\mathcal{U}^{(+)}$. Similarly, $\rho^{(-)}|_{\mathcal{P}\cap\mathcal{U}^{(-)}} = (1, 0)$ so that the moving frame map $\rho = \rho^{(-)}$ on $\mathcal{U}^{(-)}$.

The invariantization $g(\rho(z_1, z_2), z_1, z_2))$ of the coordinate functions (z_1, z_2) produces normalized invariants $(0, \sqrt{z_1^2 + z_2^2})$ on $\mathcal{U}^{(+)}$, and $(0, -\sqrt{z_1^2 + z_2^2})$ on $\mathcal{U}^{(-)}$.

Example 3.3 (Translation + reflection). The action of the Lie group $\mathcal{G} = \mathbb{R} \times \{-1, 1\}$ defined in Example 1.20 by

$$\begin{aligned} g : \mathcal{G} \times \mathbb{R}^2 &\to \mathbb{R}^2, \\ ((\lambda_1, \lambda_2), (z_1, z_2)) &\mapsto (z_1 + \lambda_1, \lambda_2 z_2), \end{aligned}$$

where $\lambda_1 \in \mathbb{R}$ and $\lambda_2 = \pm 1$, is locally free on $\mathbb{R}^2$.

In Example 2.15 we chose the algebraic cross-section $\mathcal{P}$ defined by $P = (Z_2 - Z_1)$. The corresponding moving frame ideal $M^e = (\lambda_1 - z_2\lambda_2 + z_1, \lambda_2^2 - 1)$ has two zeros $\rho^{\pm}(z_1, z_2) = (-z_1 \pm z_2, \pm 1)$. The condition that ρ produces identity of the group at the points of $\mathcal{P}$ leads to the choice $\rho(z_1, z_2) = (-z_1 + z_2, 1)$. The invariantization of the coordinate functions $g(\rho(z_1, z_2), z_1, z_2)$ produces normalized invariants (z_2, z_2).

We note that in all of the above examples we considered a one-parameter locally free action, for which a local moving frame map ρ can be easily explicitly defined, and then the invariantization map and the normalized invariants can be easily computed. The expressions for ρ often involve radicals, which provides a problem when one intends to use them to compute invariantization symbolically. Moreover, for nonlocally free actions, or even for more complicated locally free actions, finding a smooth representative for zeros of the M^e might be hard or impossible. Therefore it is computationally preferable, instead of working with ideal $M = ((Z - g(\lambda, z)) + G + P_Z) \cap \mathbb{R}[z, \lambda]$, to use the ideal $I = ((Z - g(\lambda, z)) + G + P_Z) \cap \mathbb{R}[z, Z]$, whose extension $I^e \in \mathbb{R}(z)[Z]$ leads to replacement invariants of Section 2.4, and the invariantization process and the algebraic invariantization process of Section 2.6. The theorems of the next section formalize the correspondence between the smooth and the algebraic invariantization.

3.2. *Normalized and Replacement Invariants*

Rational invariants are obviously local invariants. We show that so are smooth representatives of algebraic invariants. The following definition formalizes the notion of a smooth representative of an algebraic function.

Definition 3.4. A smooth map $F : \mathcal{U} \subset \mathcal{Z} \to \mathbb{R}^k$ is a smooth zero of a set of polynomials $\{p_1, \ldots, p_\kappa\} \subset \mathbb{R}(z)[\zeta_1, \ldots, \zeta_k]$ if the coefficients of the p_i are well defined on $\mathcal{U}$ and $p_i(\bar{z}, F(\bar{z})) = 0$ for all $\bar{z} \in \mathcal{U}$. In this case we also say that F is a smooth zero of the ideal $(p_1, \ldots, p_\kappa)$.

Proposition 3.5. *Assume $F : \mathcal{U} \to \mathbb{R}^k$ is a smooth zero of $\{p_1, \ldots, p_\kappa\} \subset \mathbb{R}(z)^G[\zeta_1, \ldots, \zeta_k]$. If $(p_1, \ldots, p_\kappa)$ is a zero-dimensional ideal, then the components of F are local invariants.*

Proof. Let $p \in \mathbb{R}(z)^G[\zeta]$, i.e., $p(z, \zeta) = \sum_{\alpha\in\mathbb{N}^n} a_\alpha(z)\zeta^\alpha$, where $a_\alpha(z) \in \mathbb{R}(z)^G$. Assume that $p(\bar{z}, F(\bar{z})) = 0$ for all $\bar{z} \in \mathcal{U}$. For any $\bar{z} \in \mathcal{U}$ and an infinitesimal generator v there exists $\varepsilon > 0$, such that $\exp(\varepsilon v, \bar{z}) \in \mathcal{U}$ whenever $|\varepsilon| < \varepsilon$. Then $p(\exp(\varepsilon v, \bar{z}), F(\exp(\varepsilon v, \bar{z}))) = \sum_{\alpha\in\mathbb{N}^n} a_\alpha(\exp(\varepsilon v, \bar{z}))F(\exp(\varepsilon v, \bar{z}))^\alpha = 0$. Since the coefficients a_α are invariant $\sum_{\alpha\in\mathbb{N}^n} a_\alpha(\bar{z})F(\exp(\varepsilon v, \bar{z}))^\alpha = 0$ for all $\bar{z} \in \mathcal{U}$ and small enough ε. Thus for a fixed point $\bar{z}$ all the values $F(\exp(\varepsilon v, \bar{z}))$ for all sufficiently small ε are the common roots of the set of polynomials $\{p_1, \ldots, p_\kappa\}$. Since by the assumption the number of roots is finite, we conclude that $F(\exp(\varepsilon v, \bar{z})) = F(\exp(0v, \bar{z})) = F(\bar{z})$ and thus the components of $F(z)$ are local invariants. □

The replacement invariants are the $\overline{\mathbb{R}(z)}^G$-zeros of the zero-dimensional ideal $I^G = (G + (Z - g(\lambda, z)) + \mathcal{P}) \cap \mathbb{R}(z)^G[Z]$. According to the previous proposition the smooth zeros of this ideal are local invariants. Such zeros exist: we show that the tuple of normalized invariants (Section 1.5) is one of those.

Theorem 3.6. *Let $\mathcal{P}$ be an algebraic cross-section which, when restricted to an open set $\mathcal{U}$, defines a local cross-section. The tuple of normalized invariants $\bar{\iota}z = (\bar{\iota}z_1, \ldots, \bar{\iota}z_n)$ is the smooth zero of the ideal I^G whose components agree with the coordinate functions on $\mathcal{P} \cap \mathcal{U}$.*

Proof. Let $\bar{z} \in \mathcal{U}$ be an arbitrary point, and let $\bar{z}_0$ be the point of intersection of $\mathcal{P}$ with the connected component of $\mathcal{O}_{\bar{z}} \cap \mathcal{U}$, containing $\bar{z}$. Then there exists $\bar{\lambda}$ in the connected component of the identity of $\mathcal{G}$, such that $\bar{z}_0 = g(\bar{\lambda}\bar{z})$ so that $(\bar{z}, \bar{z}_0)$ is a zero of the ideal $I = O + P$. By definition $\bar{\iota}z(\bar{z}) = \bar{z}_0$ and therefore $(\bar{z}, \bar{\iota}z(\bar{z}))$ is a zero of the ideal I for all $\bar{z} \in \mathcal{U}$. Equivalently, $\bar{\iota}z$ is a smooth zero of I^G. By Theorem 1.8 it is the unique tuple of local invariants that agree with the coordinate functions on $\mathcal{P} \cap \mathcal{U}$. □

Therefore the components of a replacement invariant not only generate algebraic invariants but the components of its smooth representative also generate local invariants.

Example 3.7 (Rotation). We return to Example 3.2, that extends Examples 1.17, 2.9, and 2.14, to illustrate the relation between the replacement and normalized invariants.

The replacement invariants associated to the cross-section $\mathcal{P} = \{(z_1, z_2) \mid z_2 = 0\}$ are the $\overline{\mathbb{R}(z)}^G$-zeros of the ideal $I^G = (Z_2, Z_1^2 - (z_1^2 + z_2^2))$.

The smooth maps $F^{(\pm)} : \mathbb{R}^2 \backslash \{(0, 0)\} \to \mathbb{R}^2$ s.t. $F^{(\pm)}(z_1, z_2) = (0, \pm\sqrt{z_1^2 + z_2^2})$ are smooth zeros of I^G. Their components are thus local invariants.

The manifold $\mathcal{P}$ defines a local cross-section on

$$\mathcal{U}^{(+)} = \mathbb{R}^2 \backslash \{(0, z_2) \mid z_2 < 0\} \qquad \text{or} \qquad \mathcal{U}^{(-)} = \mathbb{R}^2 \backslash \{(0, z_2) \mid z_2 > 0\}.$$

As $F^{(+)}|_{\mathcal{P}\cap\mathcal{U}^{(+)}} = (z_1, z_2)$, the tuple of normalized invariants are $(0, \sqrt{z_1^2 + z_2^2})$ on $\mathcal{U}^{(+)}$. Similarly, as $F^{(-)}|_{\mathcal{P}\cap\mathcal{U}^{(-)}} = (z_1, z_2)$, the tuples of normalized invariants are $(0, -\sqrt{z_1^2 + z_2^2})$ on $\mathcal{U}^{(-)}$.

Example 3.8 (Translation + reflection). We return to Example 3.3 that draws on Examples 1.20 and 2.15,

$$\begin{aligned} g : \mathbb{R} \times \{-1, 1\} \times \mathbb{R}^2 &\to \mathbb{R}^2, \\ (\lambda_1, \lambda_2, z_1, z_2) &\mapsto (z_1 + \lambda_1, \lambda_2\, z_2). \end{aligned}$$

with the cross-section defined by $z_2 = z_1$. In Example 2.15 we found two replacement invariants associated to $\mathcal{P}$: $\xi^{(\pm)} = (\pm z_2, \pm z_2)$. They both correspond to smooth maps $F^{(\pm)} : \mathbb{R}^2 \to \mathbb{R}^2$ the components of which are local invariants.

The manifold $\mathcal{P}$ is a local cross-section on $\mathcal{U} = \mathbb{R}^2$. Only (z_2, z_2) coincides with the coordinate functions on $\mathcal{P}$. The normalized invariants are thus (z_2, z_2).

3.3. *Smooth and Algebraic Invariantization*

In this section we link the smooth invariantization introduced in Section 1.4 and the algebraic invariantization introduced in Section 2.6. Recall that the algebraic invariantization is a map that associates a univariate polynomial over $\mathbb{R}(z)^G$ to a univariate polynomial over $\mathbb{K}[z]_{\mathcal{P}}$ (Definition 2.18).

Theorem 3.9. *Let $\mathcal{P}$ be a cross-section which, when restricted to an open set $\mathcal{U}$, defines a local cross-section. Let $f : \mathcal{U} \to \mathbb{R}$ be a smooth zero of a univariate monic squarefree polynomial $\beta \in \mathbb{K}(z)[\zeta]$. The smooth invariantization $\bar{\iota} f$ of f is a smooth zero of the algebraic $\mathcal{P}$-invariantization $\iota\beta \in \mathbb{R}(z)^G[\zeta]$ of β.*

Proof. The polynomial $\iota\beta(z, \zeta) = \sum_{i=1}^{k} b_i(z)\zeta^i$, where $b_i \in \mathbb{K}(z)^G$. Any point $\bar{z} \in \mathcal{U}$ can obtained from the point $\bar{z}_0 \in \mathcal{P}$ by a composition of flows along infinitesimal generators of the group action. The argument will not change if we assume that $\bar{z} = \exp(\varepsilon v, \bar{z}_0)$ is obtained by the flow along a single vector field. Then from the invariance of $b_i(z)$ and the local invariance of $\bar{\iota} f(z)$ it follows that, for all $\bar{z} \in \mathcal{U}$,

$$\begin{aligned} \iota\beta(\bar{z}, \bar{\iota} f(\bar{z})) &= \sum_{i=1}^{k} b_i(\exp(\varepsilon v, \bar{z}_0)) f(\exp(\varepsilon v, \bar{z}_0))^i \\ &= \sum_{i=1}^{k} b_i(\bar{z}_0)\bar{\iota} f(\bar{z}_0)^i = \iota\beta\left(\bar{z}_0, \bar{\iota} f(z_0)\right), \end{aligned}$$

where $\bar{z}_0 \in \mathcal{P} \cap \mathcal{U}$. From Proposition 2.21 it follows that $\iota\beta$ is divisible by β when restricted to $\mathcal{P}$. Thus $\iota\beta(\bar{z}_0, f(\bar{z}_0)) = 0, \forall \bar{z}_0 \in \mathcal{P} \cap \mathcal{U}$, since $\beta(\bar{z}, f(\bar{z})) \equiv 0$ on $\mathcal{U}$. It follows that $\bar{\iota} f(z)$ is a smooth zero of a polynomial $\bar{\iota}\beta(z, \zeta) \in \mathbb{K}(z)^G[\zeta]$. □

In particular, if $r(z)$ is a rational function that is well defined on $\mathcal{U}$, then its smooth invariantization $\bar{\iota}r(z)$ is a smooth zero of the $\mathcal{P}$-invariantization $\iota(\zeta - r(z))$ of the polynomial $\zeta - r(z)$. To determine the right one we only need to check that its restriction to $\mathcal{P} \cap \mathcal{U}$ coincides with $r(z)$.

4. Two Geometric Examples

We take two classical examples in differential geometry to illustrate the major points of the algebraic construction we offer. We aim here at being pedagogical by reviewing well-known cases and we reserve novel and challenging computations for future work. We first treat the action of the Euclidean group $E(2) = 0(2) \ltimes \mathbb{R}^2$ on the second-order jets of plane curves and then the action of the special affine group $SA(2) = SL(2) \ltimes \mathbb{R}^2$ on the fourth-order jets of plane curves.

Example 4.1 ($E(2)$ action on curves in $\mathbb{R}^2$). The group $E(2)$ can be defined algebraically by $G = (\alpha^2 + \beta^2 - 1, \varepsilon^2 - 1) \subset \mathbb{K}[\alpha, \beta, a, b, \varepsilon]$. The neutral element is $(1, 0, 0, 0, 1)$, the group operation $(\alpha', \beta', a', b', \varepsilon') \cdot (\alpha, \beta, a, b, \varepsilon) = (\alpha\alpha' - \beta\beta', \beta\alpha' + \alpha\beta', a + \alpha a' - \beta b', b + \alpha a' + \alpha b', \varepsilon\,\varepsilon')$, and the inverse map $(\alpha, \beta, a, b, \varepsilon)^{-1} = (\alpha, -\beta, -\alpha\, a - b\beta, \beta\, a - \alpha b, \varepsilon)$.

The variables x, y_0, y_1, y_2 stand for the independent variable, the dependent variable, its first and second derivatives, respectively.

The rational action on $\mathbb{R}^4$ we consider is given by the rational functions:

$$g_1 = \alpha x - \beta y_0 + a, \qquad g_2 = \varepsilon\beta x + \varepsilon\alpha y_0 + b,$$
$$g_3 = \varepsilon \frac{\beta + \alpha y_1}{\alpha - \beta y_1}, \qquad g_4 = \varepsilon \frac{y_2}{(\alpha - \beta y_1)^3}.$$

We consider the cross-section defined by $P = (X, Y_0, Y_1)$. The reduced Gröbner basis of the graph-section ideal $I^e = O^e + P$ is then

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

The only nontrivial coefficient, $y_2^2(1 + y_1^2)^{-3}$ is a rational invariant (Theorem 2.7). We actually recognize the square of the curvature. The curvature itself, like many other classical differential invariants, is an algebraic function. It appears as a component of a replacement invariant. Indeed, the two replacement invariants associated to the cross-section are the tuples $\xi^{(\pm)} = (0, 0, 0, \pm\kappa)$ where κ is the algebraic function defined by

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

For any rational invariant r we have the following equalities (Theorem 2.12):

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

Let $\mathcal{U} = \{((x, y_0, y_1, y_2) \in \mathbb{R}^4 \mid y_2 > 0\}$. The algebraic cross-section contains the local cross-section $\mathcal{P} = \{(x, y_0, y_1, y_2) \in \mathbb{R}^4 \mid x = y_0 = y_1 = 0, y_2 > 0\}$ for $\mathcal{U}$. The corresponding normalized invariants are

$$\bar{\iota}x = 0, \qquad \bar{\iota}y_0 = 0, \qquad \bar{\iota}y_1 = 0, \qquad \bar{\iota}y_2 = \frac{y_2}{(1+y_1^2)^{3/2}},$$

(Theorem 3.6). Thus, for any local invariant $f : \mathcal{U} \to \mathbb{R}$, we have (Theorem 1.9)

$$f(x, y_0, y_1, y_2) = f\left(0, 0, 0, \frac{y_2}{(1+y_1^2)^{3/2}}\right).$$

Example 4.2 ($SA(2)$ action on curves in $\mathbb{R}^2$). The group $SA(2)$ is defined by the ideal $G = (\alpha\delta - \beta\gamma - 1) \subset \mathbb{K}[\alpha, \beta, \gamma, \delta, a, b]$. The neutral element is $(1, 0, 0, 1, 0, 0)$, the group operation $(\alpha', \beta', \gamma'\delta', a', b') \cdot (\alpha, \beta, \gamma, \delta, a, b) = (\alpha'\alpha + \beta'\gamma, \alpha'\beta + \beta'\delta, \gamma'\alpha + \delta'\gamma, \gamma'\beta + \delta'\delta, \alpha'a + \beta'b + a', \gamma'a + \delta'b + b')$, and the inverse map $(\alpha, \beta, \gamma, \delta, a, b)^{-1} = (\delta, -\beta, -\gamma, \alpha, b\beta - a\delta, a\gamma - b\alpha)$.

The variables $x, y_0, y_1, y_2, y_2, y_4$ stand for the independent variable, the dependent variable, and up to the fourth-order derivatives of the dependent variable y_0 with respect to x.

The rational action on $\mathbb{R}^6$ we consider is given by the rational functions:

$$g_1 = \alpha x + \beta y_0 + a, \qquad g_2 = \gamma x + \beta y_0 + b,$$

$$g_3 = \frac{\delta y_1 + \gamma}{\beta y_1 + \alpha}, \qquad g_4 = \frac{y_2}{(\beta y_1 + \alpha)^3}, \qquad g_5 = \frac{\alpha y_3 + \beta(y_3 y_1 - 3y_2^2)}{(\beta y_1 + \alpha)^5},$$

$$g_6 = \frac{\beta^2(15y_2^3 - 10y_1y_2y_3 + y_1^2y_4) + \alpha\beta(2y_1y_4 - 10y_2y_3) + \alpha^2 y_4}{(\beta y_1 + \alpha)^7}.$$

We consider the cross-section defined by $P = (X, Y_0, Y_1, Y_2 - 1, Y_3)$. The reduced Gröbner basis of the graph-section ideal $I^e = O^e + P$ is then

$$\{X, Y_0, Y_1, Y_2 - 1, Y_3, Y_4^3 - r\} \qquad \text{where} \quad r = \frac{(3y_4y_2 - 5y_3^2)^3}{27y_2^8}.$$

The only nontrivial coefficient, r, is a rational invariant (Theorem 2.7). We recognize that $r = \kappa_a^3$, where κ_a is the *affine curvature*

$$\kappa_a = \frac{(y_4y_2 - \frac{5}{3}y_3^2)}{y_2^{8/3}},$$

a differential invariant that plays a central role in plane affine geometry. The affine curvature is an algebraic function. The three replacement invariants associated to the cross-section are the tuples $\xi^{(i)} = (0, 0, 0, 1, 0, \sigma_i\kappa_a)$, $1 \le i \le 3$, where

$\sigma_i \in \mathbb{C}$ are three distinct cubic roots of 1. For any rational invariant q we have the following equalities (Theorem 2.12):

$$q(x, y_0, y_1, y_2, y_3, y_4) = q(0, 0, 0, 1, 0, \sigma_i \kappa_a).$$

The normalized invariant is the only real replacement invariant:

$$\bar\iota x = 0, \quad \bar\iota y_0 = 0, \quad \bar\iota y_1 = 0, \quad \bar\iota y_2 = 1, \quad \bar\iota y_3 = 0, \quad \bar\iota y_4 = \frac{(y_4 y_2 - \frac{5}{3} y_3^2)}{y_2^{8/3}}.$$

Thus, for any local invariant $f : \mathcal{U} \to \mathbb{R}$, we have (Theorem 1.9)

$$f(x, y_0, y_1, y_2, y_3, y_4) = f\left(0, 0, 0, 1, 0, \frac{(y_4 y_2 - \frac{5}{3} y_3^2)}{y_2^{8/3}}\right).$$

Acknowledgments

We would like to thank Liz Mansfield, Peter Olver, and Agnes Szanto for discussing the ideas of the paper during the workshop “Differential Algebra and Symbolic Computation” in Raleigh, April 2004, sponsored in part by NSF grants CCR-0306406 and CCF-0347506. We are grateful to Michael Singer for continuing discussion of the project and for a number of valuable suggestions. The first author would also like to thank Jean-Baptiste Pomet for his interest and the discussions. The second author thanks Bojko Bakalov for the discussions of the paper.

References

[1] M. Ackerman and R. Hermann, *Hilbert's Invariant Theory Papers*, Vol. 8, Math. Sci. Press, Brookline, MA, 1978.

[2] T. Becker and V. Weispfenning, *Gröbner Bases—A Computational Approach to Commutative Algebra*, Springer-Verlag, New York, 1993.

[3] I. A. Berchenko and P. J. Olver, Symmetries of polynomials, *J. Symbolic Comput.* **29** (2000), 485–514.

[4] M. Boutin and G. Kemper, On reconstructing configurations of points in $\mathbb{P}^2$ from a joint distribution of invariants, *Appl. Algebra Engrg. Comm. Comput.* **15**(6) (2005), 361–391.

[5] É. Cartan, *La méthode du repère mobile*, *la théorie des groupes continus*, *et les espaces généralisés*, Exposés de Géométrie, Vol. 5, Hermann, Paris, 1935.

[6] P. Comon and B. Mourrain, Decomposition of quantics in sums of power of linear forms, *Signal Process.* **52**(2) (1996), 96–107.

[7] D. Cox, *Galois Theory*, Wiley-Interscience, New York, 2004.

[8] C. d'Andrea, T. Krick, and A. Szanto, Multivariate subresultants in roots, *J. Algebra* **302**(1) (2006), 16–36.

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

[10] H. Derksen and G. Kemper, *Computational Invariant Theory*, Invariant Theory and Algebraic Transformation Groups, Vol. I, Encyclopaedia of Mathematical Sciences, Vol. 130, Springer-Verlag, Berlin, 2002.

[11] D. Eisenbud, *Commutative Algebra with a View toward Algebraic Geometry*, Graduate Texts in Mathematics, Springer-Verlag, New York, 1994.

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

[13] R. B. Gardner, *The Method of Equivalence and its Applications*, SIAM, Philadelphia, 1989.

[14] K. Gatermann, *Computer Algebra Methods for Equivariant Dynamical Systems*, Lecture Notes in Mathematics, Vol. 1728, Springer-Verlag, Berlin, 2000.

[15] K. O. Geddes, S. R. Czapor, and G. Labahn, *Algorithms for Computer Algebra*, Kluwer Academic, Boston, MA, 1992.

[16] V. V Gorbatsecich, A. L. Onishchik, and E. B. Vinberg, *Foundations of Lie Theory and Lie Transformations Groups*, Springer-Verlag, New York, 1993.

[17] J. H. Grace and A. Young, *The Algebra of Invariants*, Cambridge University Press, Cambridge, 1903.

[18] M. L. Green, The moving frame, differential invariants and rigidity theorems for curves in homogeneous spaces, *Duke Math. J.* **45** (1978), 735–779.

[19] G.-M. Greuel and G. Pfister, *A Singular Introduction to Commutative Algebra*, Springer-Verlag, Berlin, 2002.

[20] P. A. Griffiths, On Cartan's method of Lie groups as applied to uniqueness and existence questions in differential geometry, *Duke Math. J.* **41** (1974), 775–814.

[21] G. Gurevich, *Foundations of the Theory of Algebraic Invariants*, Noordhoff, 1964.

[22] E. Hubert, Differential algebra for derivations with nontrivial commutation rules, *J. Pure Appl. Algebra* **200**(1–2) (2005), 163–190.

[23] E. Hubert and I. A. Kogan, Rational invariants of an algebraic group action. Construction and rewriting, *J. Symbolic Comput.* **42** (2007), 203–217.

[24] D. Jensen, *Higher Order Contact of Submanifolds of Homogeneous Spaces*, Lecture Notes in Mathematics, Vol. 610, Springer-Verlag, Berlin, 1977.

[25] N. Kamran, Contributions to the study of the equivalence problem of Elie Cartan and its applications to partial and ordinary differential equations, *Acad. Roy. Belg. Cl. Sci. Mém. Collect.* $8^{\circ}(2)$ **45**(7) (1989).

[26] I. A. Kogan, *Inductive Approach to Cartan's Moving Frame Method with Applications to Classical Invariant Theory*, PhD thesis, University of Minnesota, 2000.

[27] I. A. Kogan and M. Moreno Maza, Computation of canonical forms for ternary cubics, in *ISSAC*, ACM Press, New York, 2002.

[28] I. A. Kogan and P. J. Olver, Invariant Euler–Lagrange equations and the invariant variational bicomplex, *Acta Appl. Math.* **76**(2) (2003), 137–193.

[29] S. Lie, *Sophus Lie's* 1884 *differential invariant paper*, Math. Sci. Press, Brookline, MA, 1976, In part a translation of "On differential invariants" [Über Differentialinvarianten] by S. Lie [*Math. Ann.* **24** (1884), 537–578], Translated from the German by M. Ackerman, Comments and additional material by Robert Hermann, Lie Groups: History, Frontiers and Applications, Vol. III.

[30] E. L. Mansfield, Algorithms for symmetric differential systems, *Found. Computat. Math.* **1**(4) (2001), 335–383.

[31] E. L. Mansfield, *Invariant Calculus for Differential and Discrete Problems*, Cambridge University Press, Cambridge, in preparation.

[32] 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), Lecture Notes in Computer Science, Vol. 1719, pp. 392–403, Springer-Verlag, Berlin, 1999.

[33] J. L. Mundy and A. Zisserman, Editors, *Geometric Invariance in Computer Vision*, Artificial Intelligence, MIT Press, Cambridge, MA, 1992.

[34] J. L. Mundy, A. Zisserman, and D. Forsyth, Editors, *Application of Invariance in Computer Vision*, Lecture Notes in Computer Science, Springer-Verlag, Berlin, 1992.

[35] P. J. Olver, *Applications of Lie Groups to Differential Equations*, Graduate Texts in Mathematics, Vol. 107, Springer-Verlag, New York, 1986.

[36] P. J. Olver, *Equivalence*, *Invariants and Symmetry*, Cambridge University Press, Cambridge, 1995.

[37] P. J. Olver, *Classical Invariant Theory*, Cambridge University Press, Cambridge, 1999.

[38] P. J. Olver, A survey of moving frames, in H. Li, P. J. Olver, and G. Sommer, Editors, *Computer Algebra and Geometric Algebra with Applications*, Lecture Notes in Computer Science, Vol. 3519, pp. 105–138, Springer-Verlag, New York, 2005.

[39] L. V. Ovsiannikov, *Group Analysis of Differential Equations*, Academic Press, [Harcourt Brace Jovanovich] New York, 1982, Translated from the Russian by Y. Chapovsky, Translation edited by William F. Ames.

[40] A. N. Parshin and I. R. Shafarevich, Editors, *Algebraic Geometry*, *IV*, Encyclopaedia of Mathematical Sciences, Vol. 55. Springer-Verlag, Berlin, 1994.

[41] V. L. Popov and E. B. Vinberg, Invariant theory, in Parshin and Shafarevich [**40**, pp. 122–278].

[42] M. Rosenlicht, Some basic theorems on algebraic groups, *Amer. J. Math*. **78** (1956), 401–443.

[43] C. Shakiban and P. Lloyd, Signature curves statistics of DNA supercoils, in *Geometry*, *Integrability and Quantization*, pp. 203–210, Softex, Sofia, 2004.

[44] M. Spivak, *Differential Geometry*, Vol. 1, Publish or Perish, Texas, 1970.

[45] T. A. Springer, Linear algebraic groups, in Parshin and Shafarevich [**40**, pp. 1–121].

[46] B. Sturmfels, *Algorithms in Invariant Theory*, Texts and Monographs in Symbolic Computation, Springer-Verlag, Vienna, 1993.

[47] B. van der Waerden, *Modern Algebra*, 8th ed., Springer Verlag, New York, 1971.