ABSTRACT

RUDDY, MICHAEL GERARD. The Equivalence Problem and Signatures of Algebraic Curves. (Under the direction of Irina Kogan and Cynthia Vinzant).

In this thesis we study the application of the differential signature construction to the group equivalence problem for complex algebraic curves under the projective action and its subgroups. Given such an action G, a signature map assigns to a generic algebraic curve an irreducible polynomial, called the signature polynomial, with the property that two curves are G-equivalent if and only if they have the same, up to scaling, signature polynomial. We show that for any action of G, one can construct a pair of rational differential invariants, called classifying invariants, that define a signature map. Given a pair of classifying invariants, elimination algorithms allow one to straightforwardly compute a curve's signature polynomial. In practice, however, these algorithms are computationally intensive, and determination of properties of signature polynomials without their explicit computation is of interest. We derive a formula for the degree of the signature polynomial of a curve in terms of the curve's degree, the size of its symmetry group, and some quantities depending on the choice of classifying invariants. We show that for a given set of classifying invariants and a generic curve of fixed degree, the signature polynomials share the same degree, which is an upper bound. We also show that they share the same monomial support and the same genus. For the projective group and five of its subgroups (the affine, special affine, similarity, Euclidean, and special Euclidean groups), we give sets of classifying invariants and use the degree formula to derive the degree of the signature polynomial for a generic curve as a quadratic function of the curve's degree.

The Equivalence Problem and Signatures of Algebraic Curves

by
Michael Gerard Ruddy

A dissertation submitted to the Graduate Faculty of
North Carolina State University
in partial fulfillment of the
requirements for the Degree of
Doctor of Philosophy

Mathematics

Raleigh, North Carolina

2019

APPROVED BY:

Bojko Bakalov	Ernest Stitzinger
Irina Kogan Co-chair of Advisory Committee	Cynthia Vinzant Co-chair of Advisory Committee

DEDICATION

To my mother, Ana María Ruddy Romaguera.

BIOGRAPHY

The author was born in San Juan, Puerto Rico to parents Michael Palmer Ruddy and Ana María Ruddy Romaguera. At a young age he moved from Puerto Rico to the small town of Union City, Tennessee. He accidently stumbled into mathematics at the University of Tennessee at Martin, where he graduated in 2014. He then moved to Raleigh, North Carolina to attend graduate school in the Department of Mathematics at North Carolina State University. At the time of this writing, he looks forward to joining the nonlinear algebra research group at the Max Planck Institute for Mathematics in the Sciences in Leipzig, Germany as a postdoctoral researcher. Outside of teaching, learning, and discussing mathematics, the author enjoys indoor rock climbing, reading, nature, and gardening.

ACKNOWLEDGEMENTS

There are many people I wish to thank for helping me reach this point in my career and complete this work.

First, I would like to express my utmost and sincere thanks to my advisors, Irina Kogan and Cynthia Vinzant. Without the incredible amount of patience, advice, insight, and time given, I would not be the mathematician I am today, and this work would not have been possible. I could not have asked for better mentors.

I am grateful for the people at NC State who made my time there productive and enjoyable. Thank you to my committee members Bojko Bakalov and Ernert Stitzinger for your guidance. I am also very thankful to Molly Fenn for her advice and mentorship in teaching mathematics. A special thank you to the current and former staff in the mathematics department, Trisha Smith-Clinkscales, Denise Seabrooks, John Craig, and Di Bucklad, who always looked out for the graduate students.

I want to thank everyone at the nonlinear algebra semester program at ICERM who helped create such a welcoming and stimulating environment. In particular, insightful conversations with Peter Olver, Justin Chen, Danielle Brake, and Simon Telen directly contributed to ideas and work in this thesis. Thank you to my academic siblings, Faye Pasley Simon and Georgy Scholten, for providing such great support and friendship.

I want to also thank everyone who helped me reach graduate school. Thank you to all the professors in the mathematics department at UT Martin, in particular Jason DeVito, for your encouragement. I am especially thankful to my parents for instilling in me the value of education and confidence in myself, as well as providing unconditional love and support. Thank you to my mother for being such a loving and kind role model, and to my father for his advice and companionship in facing adversity.

Finally I would like to wholeheartedly thank Anila Yadavalli for her amazing support and infectious humor while we traversed the journey of graduate school together. Your work ethic and drive are a constant inspiration and have greatly motivated me during this process. You help me be the best version of myself.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

Introduction

In the view of the Felix Klein Erlangen program, geometry is the study of properties invariant under some group of transformations. For example, one can consider Euclidean geometry as the study of properties invariant under rigid motions. From this perspective, the problem of deciding equivalence of objects under a group of transformations G, is akin to asking the question: "when are two object really the 'same' with respect to some group G?" Many problems in mathematics and applications can be reformulated in this manner, and equivalence problems are closely related to many important classification problems.

In this thesis, we study the application of the differential signature construction to the equivalence problem of planar algebraic curves under the action of the projective group and its subgroups. This topic falls into both the domain of differential geometry and classical invariant theory, which studies polynomials under linear changes of variables (see [27] or [46]).

The differential signature construction originated from Cartan's method for solving equivalence problems for smooth manifolds under Lie group actions [13]. In [11], the authors proposed the use of signatures of smooth curves for object recognition, and it has subsequently been used in a variety of applications. For example, in [7] and [1] numerical schemes that approximate signatures using joint invariants are studied, and these numerical methods are used in [34] to develop a method to automatically solve jigsaw puzzles. In [24] the authors use signature curves of the contours of melanomas and benign moles to examine their global and local symmetries.

The differential signature construction for smooth planar curves consists of the following steps: (1) an action of a group on a plane is prolonged to the jet space of curves of sufficiently high order; (2) on this jet space, a pair of independent differential invariants is constructed; (3)

the restriction of this pair to a given a curve parametrizes the signature curve. In this way one can assign to each smooth curve another planar curve, the curve's signature. Since the signature curve is constructed using invariants, two G-equivalent curves will have the same signature.

In principle, a pair of independent differential invariants can always be found using the Fels-Olver moving frame method [21, 48], a modern generalization of the classical moving frame method formulated by Cartan [12]. However, these methods are local in nature; the invariants are often only locally defined and give rise to signatures which can only determine when two smooth curves contain segments that are G-equivalent. In the case of smooth curves under rigid motions, these issues are well-studied and demonstrate the challenges of using signatures to solve the group equivalence problem for smooth curves [32, 33, 44]. For analytic curves local equivalence implies global equivalence, and hence the equality of curves' signatures is sufficient to conclude that the curves are equivalent.

In the case of irreducible algebraic curves local equivalence also implies global equivalence. Therefore, when restricting to the class of algebraic curves, under some mild conditions two curves are G-equivalent if and only if they have the same signature [10]. Additionally, when the differential invariants are *rational*, the map between a curve and its signature is a rational map. In this case the signature of an irreducible algebraic curve is itself an irreducible algebraic curve, and one can use computational algebraic geometry methods such as Gröbner basis algorithms and numerical algebraic geometry to study signature curves. In particular one can use elimination to compute the *signature polynomial* of a curve, the minimal polynomial vanishing on the curve's signature.

In [10] the authors provide an elimination algorithm to compute the signature polynomial of an algebraic curve as well as study the application of signature curves to deciding whether a planar curve is the image of a given spatial curve under a central or parallel projection. In practice, elimination algorithms are computationally intensive, and directly computing signature polynomials is generally only feasible for curves of low degree. For this reason it is advantageous to determine properties of signature polynomials without their explicit computation. Not only can prior knowledge of signature curves help distinguish inequivalent curves, but it can potentially be used to construct signature polynomials and to take advantage of exciting, ongoing developments in computational algebraic geometry to study signature curves.

Given an unknown polynomial, a natural first question to ask is, "what is the polynomial's degree?" Answering this question for signature polynomials is the main focus of this thesis, but along the way we also note other interesting properties of signature polynomials. In particular we see that for a *generic* algebraic curve of fixed degree, the signature polynomials share many properties. We restrict our attention to irreducible algebraic curves and the actions of the projective group and its subgroups on the plane. Studying the curves under these actions is related to problems of classical invariant theory and also relevant to problems in image science.

Many of the results here appear in [38].

The thesis is structured as follows. In Chapter 2 we detail the group equivalence problem for curves and review some of the previous work on using differential invariants to study smooth curves under Lie group actions. We also cover some basic facts about algebraic geometry, algebraic curves, and algebraic groups, as well as prove some general results about the degree of the image of an algebraic curve under a rational map.

In Chapter 3 we first establish the existence of a rational *classifying* set of differential invariants that defines a signature map which characterizes equivalence classes of *non-exceptional* algebraic curves. We show that a generic algebraic curve is non-exceptional. We then derive a formula for the degree of the signature polynomial of a given non-exceptional algebraic curve. The chapter concludes with the study of monomial support and genus of signature polynomials of a generic algebraic curve of fixed degree and some illustrative examples.

In Chapter 4 we provide explicit sets of classifying invariants for the projective group and a selection of its subgroups. We show that one can then use the degree formula established in Chapter 3 to determine explicit upper bounds of the degree of the curve's signature polynomial, which are tight for a generic algebraic curve. We also explore the signatures of the class of algebraic curves known as Fermat curves. In Chapter 5 we discuss some future directions for exploration, including possible applications to invariant theory.

CHAPTER 2

Background

In this chapter we discuss the differential signature construction for smooth curves and cover some of the necessary algebraic geometry background with an emphasis on algebraic curves and groups.

Section 2.1 starts with a description of the group equivalence problem for curves. We then follow the classical construction of Euclidean and affine curvature using moving frames. This was generalized by Cartan to solve equivalence problems of submanifolds under Lie group actions [13]. Its modern generalization is the Fels-Olver moving frame method [21]. For planar curves under the action of a Lie group G, this method can be used to construct G-invariant curvature, which is the starting point for the differential siganture construction for smooth curves [11]. We discuss this construction and how it can be used to study the group equivalence for smooth curves.

The next section covers some introductory algebraic geometry, highlighting Bezout's theorem and Bertini's theorem on smoothness and their role in studying the intersection mutliplicities of algebraic curves. We use both of these theorems to prove results about the degree of the image of an irreducible algebraic curve under a rational map. Finally we conclude with some basic facts about algebraic groups and the associated ring of rational invariants. In Section 2.3.1 we introduce the main group actions of study in Chapter 4: the action of the projective, affine, special affine, similarity, Euclidean, and special Euclidean groups on $\mathbb{C}^2$.

2.1 Equivalence problem and differential signatures

Definition 2.1.1. A map $\Phi : G \times S \to S$ defines an **action** of the group G on the set S if it satisfies the following two properties:

1. $\Phi(e, p) = p$, for all $p \in S$, where e is the identity in G, and
2. $\Phi(h, \Phi(g, p)) = \Phi(h \cdot g, p)$, for all $h, g \in G$ and $p \in S$.

We use the following abbreviation $\Phi(g, p) = g \cdot p$ for the action when the context is clear.

Definition 2.1.2. A group G is a **Lie group** if G is a smooth manifold, and the group multiplication and inverse maps are smooth.

Definition 2.1.3. A group G is an **algebraic group** if G is an algebraic variety, and the group multiplication and inverse maps are regular maps.

A smooth manifold is a topological space that is locally diffeomorphic to Euclidean space (for a precise definition see [42, pg. 13]). We review the definitions of an algebraic variety and regular maps in Section 2.2.

Definition 2.1.4. A map between sets $f : S \to R$ is **invariant** under the action of G on S if $f(g \cdot p) = f(p)$ for all $p \in S, g \in G$. If R is a field, we call f an **invariant function**.

In this thesis, we will mainly be concerned with the actions of these two types of groups: Lie groups and algebraic groups. For each, we impose certain restrictions on the set S and the group action map Φ. While we define many of the following objects generally, it is helpful to keep in mind the motivating cases of the actions of Lie and algebraic groups.

Group G	Set S	Action Φ	Invariants I
Lie group	Smooth manifolds	Smooth map	Smooth functions
Algebraic group	Varieties	Rational map	Polynomial/rational functions

If S is topological space and G is a topological group (see [42, pg. 151]) we can consider the *local action* of G on S.

Definition 2.1.5. A topological group G **acts locally** on a topological space S via the map $\Phi : \Omega \to S$ if $\Omega \supset \{e\} \times S$ is an open subset of $G \times S$ and Φ satisfies

1. $\Phi(e, p) = p$, for all $p \in S$ and
2. $\Phi(h, \Phi(g, p)) = \Phi(h \cdot g, p)$, for all $p \in S$ and $g, h \in G$ such that (g, p) and $(h \cdot g, p)$ lie in Ω.

Remark 2.1.6. The rational action of an algebraic group on a variety, when the base field is $\mathbb{R}$ or $\mathbb{C}$, is a specific instance of the local action of a Lie group. Here open subsets are defined by the Zariski-topology, but an algebraic group can still be given a smooth structure of a Lie group [52, Ch. 3, Sec. 2.1.2].

As we are primarily concerned with this scenario, we limit discussion to this special case (see Section 2.3). In the smooth case, we consider examples of globally defined actions on Euclidean space, namely subgroups of the general linear group of real matrices $\mathcal{GL}(n, \mathbb{R})$.

Example 2.1.7. The group of $n \times n$ invertible matrices is the *general linear group* $\mathcal{GL}(n, \mathbb{R})$. The natural action of $\mathcal{GL}(n, \mathbb{R})$ on $\mathbb{R}^n$ is given by $A \cdot x$ for $A \in \mathcal{GL}(n, \mathbb{R})$ and $x \in \mathbb{R}^n$.

Considering the action of G on a particular element $p \in S$, yields two important sets, the *stabilizer* and the *orbit* of p. The former denotes the set of elements of G that fix p, and the latter the image of the map $\Phi : G \to S$ defined by $\Phi(g) = \Phi(g, p)$.

Definition 2.1.8. For an action of G on a set S and an element $p \in S$, the **stabilizer of** p is a subgroup of G given by

$$G_p = \{g \in G \,|\, g \cdot p = p\},$$

while the **orbit of** p is the set

$$Gp = \{q \in S \,|\, \exists g \in G, g \cdot p = q\}.$$

An action is said to be **transitive** if there is only one orbit, i.e. $Gp = S$ for all $p \in S$.

Definition 2.1.9. The action of G on S is said to be **effective** if $G_S = \cap_{p \in S} G_p = \{e\}$ and **free** if $G_p = \{e\}$ for all $p \in S$.

In other words an action is effective if the only element of G that fixes each element S is the identity and free if the only element of G that fixes any element of S is the identity. Clearly a free action is also effective.

Particularly important are maps on the space that are invariant (Definition 2.1.4) or equivariant under the action of G. Note that invariant maps are necessarily constant on the orbits of G in S.

Invariant functions are useful in determining equivalence under the action of G, as for any two points $p, q \in S$ if $f(p) \neq f(q)$ then p and q lie in different orbits. However $f(p) = f(q)$ does not in general imply that p and q lie in the same orbit. A set of invariants that has this property is called *separating*.

Definition 2.1.10. A set of invariants $\mathcal{I} = \{f_1, \ldots, f_s\}$ is **separating on a subset** $U \subset S$ for the action of G on S if for any $p, q \in U$,

$$q \in Gp \;\; \Leftrightarrow \;\; f_i(p) = f_i(q), \;\; i = 1, \ldots, s.$$

Definition 2.1.11. For the action of G on sets S and R, a G**-equivariant map** $f : S \to R$ is a map such that the following diagram commutes:

$$\begin{array}{ccc} R & \xrightarrow{g\cdot} & R \\ {\scriptstyle f}\uparrow & & \uparrow{\scriptstyle f} \\ S & \xrightarrow{g\cdot} & S \end{array}$$

Example 2.1.12. The subgroup of $\mathcal{GL}(2, \mathbb{R})$ of orthogonal matrices with determinant one,

$$\mathcal{SO}(2, \mathbb{R}) = \left\{ \left[\begin{array}{cc} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{array} \right] \;\middle|\; \theta \in \mathbb{R} \right\},$$

has an effective an action on $\mathbb{R}^2$ defined by the map

$$\Phi(g, x, y) \mapsto (\cos(\theta)x + \sin(\theta)y, -\sin(\theta)x + \cos(\theta)y).$$

The group $\mathcal{SO}(2, \mathbb{R})$ is isomorphic to the group of rotations of $\mathbb{R}^2$. The set of orbits of the action consists of the origin along with circles centered at the origin, and hence is not transitive. This action is effective on $\mathbb{R}^2$ and free on the subset $\mathbb{R}^2 \backslash \{(0, 0)\}$.

The function on $\mathbb{R}^2$ given by $f(x, y) = x^2 + y^2$ is an invariant function for the action of $\mathcal{SO}(2, \mathbb{R})$. It is also *fundamental* in the sense that any other invariant for this action can be written as a smooth function of f. This invariant is also separating; two points lie in the same orbit if and only if they have the same image under f.

Example 2.1.13. The subgroup of $\mathcal{GL}(3, \mathbb{R})$,

$$\mathcal{SE}(2, \mathbb{R}) = \left\{ \left[\begin{array}{ccc} \cos(\theta) & \sin(\theta) & a \\ -\sin(\theta) & \cos(\theta) & b \\ 0 & 0 & 1 \end{array} \right] \;\middle|\; a, b, \theta \in \mathbb{R} \right\},$$

has an effective an action on $\mathbb{R}^2$ defined by the map

$$\Phi(g, x, y) \mapsto (\cos(\theta)x + \sin(\theta)y + a, -\sin(\theta)x + \cos(\theta)y + b).$$

The group $\mathcal{SE}(2, \mathbb{R})$ is isomorphic to the group of orientation-preserving rigid motions of the real plane, called the *special Euclidean group of transformations* of $\mathbb{R}^2$, which is generated by rotations and translations of the plane.

Example 2.1.14. The subgroup of $\mathcal{GL}(3,\mathbb{R})$,

$$\mathcal{SA}(2,\mathbb{R}) = \left\{ \begin{bmatrix} a_1 & a_2 & a_3 \\ a_4 & a_5 & a_6 \\ 0 & 0 & 1 \end{bmatrix} \middle| \; a_1a_5 - a_2a_4 = 1, a_i \in \mathbb{R}, 1 \leq i \leq 6 \right\},$$

has an effective an action on $\mathbb{R}^2$ defined by the map

$$\Phi(g, x, y) \mapsto (a_1x + a_2y + a_3, a_4x + a_5y + a_6).$$

The group $\mathcal{SA}(2,\mathbb{R})$ is isomorphic to the group of area-preserving transformations of $\mathbb{R}^2$, known as the *special affine group*.

The actions on $\mathbb{R}^2$ defined in Examples 2.1.13 and 2.1.14 on are transitive, and hence the only invariant maps on $\mathbb{R}^2$ are constant.

Classical invariant theory was concerned with determining equivalence classes of homogeneous polynomials under a linear change of variables, as well as computing generating sets of the ring of polynomial invariants and the field of rational invariants for this action [46]. The next example is a simple illustration of a problem of this type.

Example 2.1.15. A conic in $\mathbb{R}^2$ is given by the zero set of the polynomial

$$F(x, y) = a_{20}x^2 + a_{11}xy + a_{02}y^2 + a_{10}x + a_{01}y + a_{00}, \tag{2.1}$$

where $a_{ij} \in \mathbb{R}$, $0 \leq i, j \leq 2$. Any linear change of coordinates preserves the degree of a polynomial, and thus sends conics to conics. In particular, we can consider the action of $\mathcal{SE}(2,\mathbb{R})$ on the space of such polynomials. The polynomial F can be represented as a matrix where

$$F(x, y) = \begin{bmatrix} x & y & 1 \end{bmatrix} A \begin{bmatrix} x \\ y \\ 1 \end{bmatrix},$$

where

$$A = \begin{bmatrix} a_{20} & a_{11}/2 & a_{10} \\ a_{11}/2 & a_{02} & a_{01}/2 \\ a_{10}/2 & a_{01}/2 & a_{00} \end{bmatrix}.$$

Then for $g \in \mathcal{SE}(2,\mathbb{R})$ the action can be defined as

$$\begin{aligned}\overline{F}(x,y) &= F(g\cdot(x,y)) \\ &= \begin{bmatrix} \cos(\theta)x+\sin(\theta)y+a \\ -\sin(\theta)x+\cos(\theta)y+b \\ 1 \end{bmatrix}^T A \begin{bmatrix} \cos(\theta)x+\sin(\theta)y+a \\ -\sin(\theta)x+\cos(\theta)y+b \\ 1 \end{bmatrix} \\ &= \begin{bmatrix} x & y & 1 \end{bmatrix} \overline{A} \begin{bmatrix} x \\ y \\ 1 \end{bmatrix}.\end{aligned}$$

Denote the upper left 2x2 submatrix of A as B. One can check that the functions $\det(A)$, $\det(B)$, and $\mathrm{tr}(B)$ are invariant under the action of $\mathcal{SE}(2,\mathbb{R})$. We will show that $\mathcal{I} = \{\det(A), \det(B), \mathrm{tr}(B)\}$ is a separating set of invariants on the Zariski-open subset defined by $\det(B) \neq 0$. Let $F(x,y)$ be any conic where $\det(B) \neq 0$. Apply the transformation g to $F(x,y)$, given by

$$(x,y) \mapsto \left(x + \frac{a_{11}a_{01} - 2a_{02}a_{10}}{4\det(B)}, y + \frac{a_{11}a_{10} - 2a_{20}a_{01}}{4\det(B)} \right),$$

which yields

$$F(g\cdot(x,y)) = \overline{F}(x,y) = a_{20}x^2 + a_{11}xy + a_{02}y^2 + \mu,$$

where $\mu = \frac{\det(A)}{\det(B)}$. Since B is a symmetric real matrix, for some $\theta \in \mathbb{R}$, we can write

$$\begin{bmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{bmatrix} \cdot B \cdot \begin{bmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{bmatrix} = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix},$$

where $\lambda_1 \geq \lambda_2$, which corresponds to the action of a rotation $g \in \mathcal{SE}(2,\mathbb{R})$ such that $\overline{F}(g\cdot(x,y)) = \tilde{F}(x,y)$ where

$$\tilde{F}(x,y) = \lambda_1 x^2 + \lambda_2 y^2 + \mu. \tag{2.2}$$

The values λ_1, λ_2 are the zeros of the characteristic equation

$$\lambda^2 - \mathrm{tr}(B)\lambda + \det(B) = 0.$$

Thus any polynomial of the form (2.1) where $\det(B) \neq 0$ can be transformed to the form (2.2) by a transformation in $\mathcal{SE}(2,\mathbb{R})$, where λ_1, λ_2, and μ are completely determined by the values of $\det(A), \det(B)$, and $\mathrm{tr}(B)$. Thus for two polynomials F_1 and F_2 where $\det(B_1), \det(B_2) \neq 0$, if

$$\det(A_1) = \det(A_2), \quad \det(B_1) = \det(B_2), \quad \mathrm{tr}(B_1) = \mathrm{tr}(B_2)$$

they must lie in the same orbit, showing that $\mathcal{I}$ is separating. The set of invariants $\mathcal{I}$ is not separating for such polynomials where $\det(B) = 0$. Consider

$$F_1(x, y) = x^2 + x$$
$$F_2(x, y) = x^2 + 2x.$$

We can evaluate the invariants in $\mathcal{I}$ for each:

$$\det(A_1) = \det(A_2) = 0 \det(B_1) = \det(B_2) \qquad = 0 \mathrm{tr}(B_1) = \mathrm{tr}(B_2) = 1$$

Thus the polynomials take the same values for each invariant in $\mathcal{I}$, however, one can check that they are not equivalent under $\mathcal{SE}(2, \mathbb{R})$.

2.1.1 Equivalence problem for curves and classical moving frames

Given the action of a group G on the real or complex plane, there is an induced action on the set of planar curves.

Definition 2.1.16. Two curves X and X' are said to be G**-equivalent**, under a group G acting on the curve's ambient space, if there exists $g \in G$ such that $g \cdot X = X'$. We denote this $X \cong_G X'$.

In this language the *equivalence problem for curves* can be stated as: given two curves X and X', determine if they are G-equivalent.

Example 2.1.17. Consider the action of $\mathcal{SE}(2, \mathbb{R})$ on $\mathbb{R}^2$ defined in Example 2.1.13. Each element of $\mathcal{SE}(2, \mathbb{R})$ is an automorphism of $\mathbb{R}^2$, and thus maps curves to curves. The question, 'When are two curves related by a rigid motion?' can be translated to 'When are two curves $\mathcal{SE}(2, \mathbb{R})$-equivalent?'

The elements of G that map X to itself are the self-equivalences or symmetries of X and form a subgroup of G.

Definition 2.1.18. The **symmetry group** of X under G is given by the subgroup

$$\mathrm{Sym}(X, G) = \{g \in G \,|\, g \cdot X = X\}.$$

While many of the group actions on $\mathbb{R}^2$ are transitive, in the smooth case, the space of curves is infinite-dimensional. However, the equivalence problem can be studied in finite dimensional jet space, by considering the action of $\mathcal{SE}(2,\mathbb{R})$ on the derivatives of a curve. This is a topic of classical differential geometry. In this section we will review the classical construction of a Frenet frame for the action of $\mathcal{SE}(2,\mathbb{R})$ to derive the invariant Euclidean curvature and discuss some of its generalizations.

Here we will refer to a curve X in the plane as *smooth* if there exists a smooth function $\gamma : I \to \mathbb{R}^2$ for some interval $I \subset \mathbb{R}$ where $X = \gamma(I)$. We say that $\gamma(t)$ is a *parameterization* of the curve X. If $\tilde{\gamma}(t) : I' \to I$ is any diffeomorphism between intervals of $\mathbb{R}$, then $X = \gamma(\tilde{\gamma}(I'))$, and hence $\gamma(\tilde{\gamma}(t))$ defines the same curve. From this one can see that for any curve X, there are infinitely many parameterizations of X. For this reason, it is useful to choose a particular representative from the set of parameterizations of a curve X.

Since we are considering curves under $\mathcal{SE}(2,\mathbb{R})$, we choose a parameterization that is preserved under translations and rotations of the curve.

Definition 2.1.19. The parameterization $\gamma : [0, L] \to \mathbb{R}^2$ defined by $\gamma(s) = (x(s), y(s))$ is said to an **arc length parameterization** of a curve X if the tangent vector $\gamma'(s) = (x'(s), y'(s))$ is always a unit vector, i.e. $\sqrt{x'(s)^2 + y'(s)^2} = 1$ for all $s \in [0, L]$.

The requirement that the curve's tangent vector be a unit vector is a property that is preserved under the action of $\mathcal{SE}(2,\mathbb{R})$ on the curve. This is an immediate consequence of the fact that interpoint distance is a Euclidean invariant. Note that if γ is an arbitrary parameterization of a curve then

$$s = \int_0^\tau |\gamma'(\tau)| d\tau.$$

Remark 2.1.20. Given an initial point (x_0, y_0) on a directed, smooth curve X, there is unique arc length parameterization $\gamma(s)$ such that $\gamma(0) = (x_0, y_0)$ and $\gamma(s)$ traces out the curve exactly once. The choice of initial point and direction are important, as a closed smooth curve may have infinitely many different arc length parameterizations and two different arc length parameterizations with the same initial point.

A planar Cartesian system of coordinates is defined by a point and two orthonormal vectors. For example, the origin $(0, 0)$ and the basis for $\mathbb{R}^2$ given by $\{e_1, e_2\} = \{(1, 0), (0, 1)\}$ are the standard choices for a planar system of coordinates. At each point of a smooth curve $\gamma(s) \in X$ parameterized by arc length, the unit tangent vector $T(s) = (x'(s), y'(s))$ and the unit normal vector $N(s) = (-y'(s), x'(s))$ define a system of coordinates with $f(s)$ as the new origin and new axes defined by $T(s)$ and $N(s)$.

Thus at each point of the curve X, there exists a basis that changes as one moves along the curve, known as the classical Frenet frame. This system of coordinates is uniquely determined by a rotation and translation of the vectors $\{e_1, e_2\}$. The frame matrix given by

$$A(s) = \begin{bmatrix} x'(s) & y'(s) \\ -y'(s) & x'(s) \end{bmatrix} \tag{2.3}$$

takes the basis $\{e_1, e_2\}$ to $\{T(s), N(s)\}$, i.e. $\begin{bmatrix} T(s) \\ N(s) \end{bmatrix} = A(s) \begin{bmatrix} e_1 \\ e_2 \end{bmatrix}$. Note that, for an arc length parametrization, the derivative of the tangent vector $T'(s) = (x''(s), y''(s))$ is orthogonal to $T(s)$, and thus parallel with $N(s)$. Similarly $N'(s)$ is orthogonal to $N(s)$ and hence parallel with $T(s)$. The relationship between the basis $\{T'(s), N'(s)\}$ and $\{T(s), N(s)\}$ is given by

$$\begin{bmatrix} T'(s) \\ N'(s) \end{bmatrix} = A'(s) = A'(s)A^{-1}(s)A(s) = A'(s)A^{-1}(s) \begin{bmatrix} T(s) \\ N(s) \end{bmatrix}, \tag{2.4}$$

where

$$A'(s)A^{-1}(s) = \begin{bmatrix} 0 & x'(s)y''(s) - y'(s)x''(s) \\ -x'(s)y''(s) + y'(s)x''(s) & 0 \end{bmatrix} = \begin{bmatrix} 0 & \kappa(s) \\ -\kappa(s) & 0 \end{bmatrix}.$$

Thus, from above and (2.4), $\kappa(s)$ is the function satisfying the Frenet equations

$$\begin{aligned} T'(s) &= \kappa(s)N(s) \\ N'(s) &= -\kappa(s)T(s). \end{aligned}$$

The function $\kappa(s)$ is known as the *Euclidean curvature* and is a differential invariant for the action of $\mathcal{SE}(2, \mathbb{R})$ on curves. For an arbitrary parameterization $\gamma(t)$ of a curve the Euclidean curvature is given by

$$\kappa(t) = \frac{x'(t)y''(t) - y'(t)x''(t)}{(x'(t)^2 + y'(t)^2)^{3/2}}.$$

Euclidean curvature generates the algebra of differential invariants in the following sense:

Theorem 2.1.21. Any differential invariant of planar curves under the action of $\mathcal{SE}(2, \mathbb{R})$ can be written as a smooth function of Euclidean curvature and its derivatives with respect to arc length.

Euclidean curvature also provides a way of establishing $\mathcal{SE}(2,\mathbb{R})$-equivalence:

Theorem 2.1.22. If two smooth curves have the same Euclidean curvature as a function of arc length, then they are $\mathcal{SE}(2,\mathbb{R})$-equivalent.

The above two theorems can be found in [25].

Remark 2.1.23. The converse of Theorem 2.1.22 does not always hold. As discussed in Remark 2.1.20 the *same* curve X may have many different arc length parameterizations, and hence different Euclidean curvatures as a function of arc length. This parameterization depends on the initial point chosen, as well as the direction if X is a closed curve. Later we discuss the construction of a *signature* in Section 2.1 which avoids these issues.

Similarly we can define a frame for the action of the special affine group $\mathcal{SA}(2,\mathbb{R})$ (see Example 2.1.14) on $\mathbb{R}^2$. The arc length parameterization of a curve is not invariant under all transformations $g \in \mathcal{SA}(2,\mathbb{R})$ since distance is not preserved under the action of $\mathcal{SA}(2,\mathbb{R})$.

This action does, however, preserve area. One can instead choose a parameterization $\gamma(t)$ such that the parallelogram defined by the vectors $\gamma'(t)$ and $\gamma''(t)$ has unit area. In other words a parameter α, known as *affine arc length* such that

$$|\gamma'(\alpha) \times \gamma''(\alpha)| = 1, \tag{2.5}$$

where $\times$ denotes cross product. This corresponds to the parallelogram defined by $\gamma'(\alpha)$ and $\gamma''(\alpha)$ having unit area. Here the frame matrix is given by $A(\alpha) = \begin{bmatrix} \gamma'(\alpha) \\ \gamma''(\alpha) \end{bmatrix}$. Then the matrix

$$A'(\alpha)A^{-1}(\alpha) = \begin{bmatrix} 0 & 1 \\ -(x''(\alpha)y'''(\alpha) - x'''(\alpha)y''(\alpha)) & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -\mu(\alpha) & 0 \end{bmatrix}$$

has the property that

$$\begin{bmatrix} \gamma'(\alpha) \\ \gamma'''(\alpha) \end{bmatrix} = A'(\alpha)A^{-1}(\alpha) \begin{bmatrix} \gamma'(\alpha) \\ \gamma''(\alpha) \end{bmatrix}.$$

The function $\mu(\alpha)$ is the *affine curvature* of X and is a differential invariant for the action of $\mathcal{SA}(2,\mathbb{R})$ on curves [6]. For an arbitrary parameterization $\gamma(t)$ the affine curvature is given by

$$\mu(t) = \frac{-(5/9)(x'(t)y'''(t) - x'''(t)y'(t))^2}{(x'(t)y''(t) - x''(t)y'(t))^{8/3}} + \frac{(x''(t)y'''(t) - x'''(t)y''(t)) + (x'(t)y'''(t) - x'''(t)y'(t))}{(x'(t)y''(t) - x''(t)y'(t))^{5/3}}.$$

As in the Euclidean case, the following theorems hold for affine curvature and affine arc length (See [46, Ex. 8.48] and [25, Thm. 7-27] respectively).

Theorem 2.1.24. Any differential invariant of planar curves under the action of $\mathcal{SA}(2,\mathbb{R})$ can be written as a smooth function of affine curvature and its derivatives with respect to affine arc length.

Theorem 2.1.25. If two smooth curves have the same affine curvature as a function of affine arc length, then they are $\mathcal{SA}(2,\mathbb{R})$-equivalent.

This frame construction was generalized by Cartan to solve a variety of equivalence problems of submanifolds of varying dimension [13]. Using this method one can show that for planar curves under any smooth, transitive action of a Lie group there exists a similar notion of G-invariant arc length and G-invariant curvature [46].

Theorem 2.1.26. Let G be an ordinary[1] Lie group acting smoothly on $\mathbb{R}^2$. Then there exists an invariant parameter s, called *G-invariant arc length*, and a differential invariant $\kappa(s)$, called *G-invariant curvature*, such that any differential invariant of planar curves under G can be written as a smooth function of $\kappa(s)$ and its derivatives with respect to s.

Note that the Euclidean frame $\{T(s), N(s)\}$ centered at a point $f(s)$ on the curve X is completely determined by a translation and rotation of the standard basis $\{e_1, e_2\}$ centered at the origin. A rotation and translation of X also rotates and translates the frame.

In this way we can view the Frenet frame an as an $\mathcal{SE}(2,\mathbb{R})$-equivariant map from X to $\mathcal{SE}(2,\mathbb{R})$ for the action of $\mathcal{SE}(2,\mathbb{R})$ on X and on itself via left multiplication. The frame defined by $A(\alpha)$ at a point $\gamma(\alpha)$ similarly defines an $\mathcal{SA}(2,\mathbb{R})$-equivariant map from X to $\mathcal{SA}(2,\mathbb{R})$.

In [21] Fels and Olver generalized Cartan's method to any smooth action of a finite-dimensional Lie group G on a manifold M by defining a *moving frame* as a G-equivariant map from M into G. With a moving frame map in hand, one can then use a *cross-section* (a submanifold that transversely intersects each orbit exactly once) to the orbits of G to construct a generating set of local invariants for the action of G on M. For an algebraic formulation of the Fels-Olver construction see [35].

2.1.2 Differental signature curves

In the previous section we saw issues with using G-invariant curvature to study the equivalence problem. Choice of two different initial points will result in two G-invariant curvatures as functions of G-invariant arc length, related by translation. Additionally, computing G-invariant arc length often requires (usually non-trivial) integration.

[1] Most smooth actions on the plane, including all the ones considered in this thesis, are ordinary. For a precise definition see [46, pg. 175]

Definition 2.1.27. For a smooth curve X the **signature curve** of X with respect to the action of G is the curve $\mathcal{S}_X$ parameterized by (K_1, K_2), where K_1 and K_2 are functionally independent differential invariants for the action of G on $\mathbb{R}^2$. We call the map $\sigma_X : X \to \mathcal{S}_X$, defined by $\sigma_X = (K_1, K_2)$, the **signature map** of X with respect to the action of G.

In [11], the authors introduced the notion of a *signature curve* using $K_1 = \kappa$, G-invariant curvature, and $K_2 = \kappa_s$, the derivative of κ with respect to G-invariant arc length. This gives a method to study the equivalence problem for plane curves while avoiding the issues mentioned above. The signature curve is a special case of the classifying manifold introduced by Cartan [13]. For most actions of a Lie Group G on $\mathbb{R}^2$, Theorem 2.1.26 guarantees the existence of the two invariants κ and κ_s.

Two G-equivalent curves will clearly have the same signature curve, as the signature map is constructed using differential invariants for the action of G. The converse of this statement is true only under certain regularity conditions (see [11]), which are not satisfied by closed curves. The most one can say about two smooth curves with equal signatures is that there exists a segment of one curve G-equivalent to a segment of the other curve.

In the case of analytic and algebraic curves, this local equivalence is enough to establish global equivalence. For a given group of transformations G, determining the set of smooth curves for which their signature curves establish global equivalence is an open problem. In [44] and [32], the authors explored this question for $G = \mathcal{SE}(2, \mathbb{R})$, and it was shown that an infinite family of smooth curves could be constructed with equal Euclidean signatures, none of which were $\mathcal{SE}(2, \mathbb{R})$-equivalent. It was noted that curve segments of constant curvature, such as straight lines or circular arcs, could be inserted in smooth curves without changing the curve's Euclidean signature.

Example 2.1.28. For the action of the special Euclidean group $\mathcal{SE}(2, \mathbb{R})$ on $\mathbb{R}^2$, G-invariant curvature and arc length are given by the familiar notions of Euclidean curvature and arc length. Euclidean curvature and its derivative with respect to arc length define the signature map $\sigma_X^{\mathcal{SE}} = (\kappa, \kappa_s)$ from the curve X to its *Euclidean signature*, which we denote $\mathcal{S}_X^{\mathcal{SE}}$. Similarly affine curvature and its derivative with respect to affine arc length define the signature map $\sigma_X^{\mathcal{SA}} = (\mu, \mu_\alpha)$ for the action of $\mathcal{SA}(2, \mathbb{R})$.

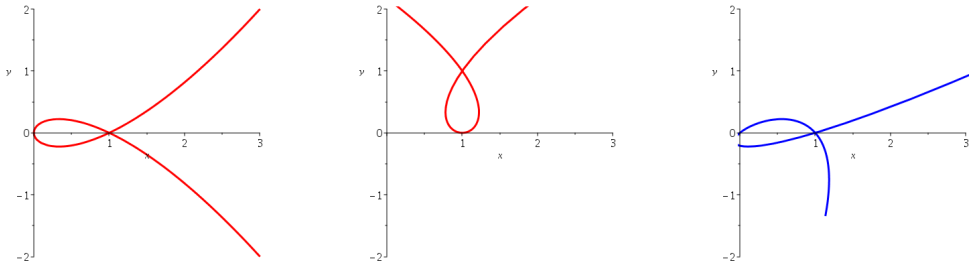

Figure 2.1: Three algebraic curves.

In Figure 2.1 are three algebraic curves; the two curves in red are clearly $\mathcal{SE}(2,\mathbb{R})$-equivalent, while the curve in blue is inequivalent to either of the red curves. However, all three curves are equivalent under the action of $\mathcal{SA}(2,\mathbb{R})$. In Figture 2.2 each curve's Euclidean and special affine signature is plotted. The Euclidean signature distinguishes the blue from the red curves. Since the curves are algebraic, equality of the red curves' signature is enough to guarantee equivalence. Similarly all the equality of all three curves' special affine signatures imply they are all $\mathcal{SA}(2,\mathbb{R})$-equivalent.

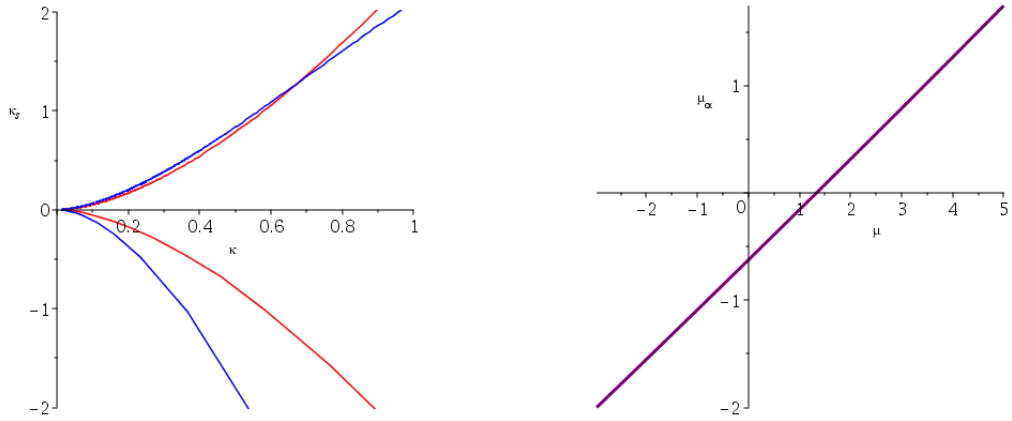

Figure 2.2: The Euclidean and special affine signatures respectively of the curves in Figure 2.1.

A useful property of signature curves is that curves with 'close' signature curves often are 'almost equivalent.' How to best formally define 'close' and 'almost equivalent,' i.e. develop a metric on signature curves and equivalence classes of curves, is an open question. However, in practice, signature curves perform well under noise when appropriate smoothing is applied as evidenced in [33, 34].

The signature curve for smooth curves does, however, contain more information than local G-equivalence. The next theorem, which appears in [11], shows that the dimension of the image of the signature map characterizes curves with finite symmetry groups.

Theorem 2.1.29. A curve X has constant G-invariant curvature if and only if $\mathrm{Sym}(X, G)$ has positive dimension. In this case the signature curve of X with respect to G is zero-dimensional.

2.2 Algebraic Geometry

Algebraic geometry can be thought of as the study of polynomial systems and the geometric objects they define. In this section we will introduce some of the basic objects of study in algebraic geometry and some results specific to algebraic curves. Here $\mathbb{K}$ will denote an arbitrary field of characteristic zero, which we do not assume to be algebraically closed unless otherwise stated. For a more in-depth, introductory treatment of this topic see [17], [30], or [50].

Definition 2.2.1. The **ring of polynomials** in $x_1, \ldots, x_n$ with coefficients in $\mathbb{K}$ is denoted $\mathbb{K}[x_1, \ldots, x_n]$. For any finite collection of polynomials $F_1, \ldots, F_s \in \mathbb{K}[x_1, \ldots, x_n]$, we denote the **ideal generated by** $F_1, \ldots, F_s$ as $\langle F_1, \ldots, F_s \rangle$.

Remark 2.2.2. We will denote the collection of n-tuples of elements of $\mathbb{K}$ as $\mathbb{K}^n$ or *n-dimensional affine space*. The name affine emphasizes that we are concerned with the geometric properties of $\mathbb{K}^n$, rather than its properties as a vector space with a designated origin.

Note that any point lying in the zero set of $\{F_1, \ldots, F_s\}$ (i.e. the points $p \in \mathbb{K}^n$ such that $F_1(p) = F_2(p) = \ldots = F_s(p) = 0$) also lies in the zero set of $H \in \langle F_1, \ldots, F_s \rangle$. Thus there is a natural identification of the zero set of a collection of polynomials with the ideal they generate.

Definition 2.2.3. A **variety** is a subset $X \subset \mathbb{K}^n$ such that there exists a collection of polynomials $\{F_1, \ldots, F_s\}$ where X is the set of points where $F_1, \ldots, F_s$ all vanish, which is denoted $V(F_1, \ldots, F_s)$. The variety of a collection of polynomials $\{F_1, \ldots, F_s\}$ is the set $V(F_1, \ldots, F_s)$.

If $I = \langle F_1, \ldots, F_s \rangle$, one can check that $V(F_1, \ldots, F_s) = V(I)$.

Definition 2.2.4. For a set $S \subset \mathbb{K}^n$, the **ideal of polynomials vanishing on** S is defined

$$\mathcal{I}(S) = \{F \in \mathbb{K}[x_1, \ldots, x_n] \mid F(s) = 0, \text{ for all } s \in S\}.$$

By the Hilbert Basis Theorem [30, pg. 19], which states that every ideal of $\mathbb{K}[x_1, \ldots, x_n]$ is finitely generated, for any $S \subset \mathbb{K}^n$ we can write $\mathcal{I}(S) = \langle F_1, \ldots, F_s \rangle$ for some $F_i \in \mathbb{K}[x_1, \ldots x_n], i = 1, \ldots, s$. Note that many subsets $S \subset \mathbb{K}^n$ are not varieties, and hence, S is often a proper subset of $V(\mathcal{I}(S))$.

Example 2.2.5. Taking $\mathbb{K} = \mathbb{R}$, consider any infinite, proper subset $S \subset \mathbb{R}$. Then any polynomial $F \in \mathbb{R}[x]$ vanishing on S has infinitely many roots, and hence $\mathcal{I}(S) = \langle 0 \rangle$. Since $V(\langle 0 \rangle) = \mathbb{R}$, clearly $S \neq V(\mathcal{I}(S))$.

The set of varieties in $\mathbb{K}^n$ define a topology called the *Zariski-topology* on affine space [30].

Proposition 2.2.6. The set of Zariski closed subsets of $\mathbb{K}^n$ define a topology on $\mathbb{K}^n$, i.e.

1. $\emptyset, \mathbb{K}^n$ are Zariski closed.
2. If S_1, S_2 are Zariski closed, then $S_1 \cup S_2$ is Zariski closed.
3. Any countable intersection of Zariski closed sets is Zariski closed.

The smallest variety containing S is called the *Zariski closure of* S and is denoted $\overline{S}$. Thus we can say that $V(\mathcal{I}(S)) = \overline{S}$. Unless otherwise stated, when we refer to the closure of a set, we mean its Zariski closure.

Definition 2.2.7. A variety is said to be **irreducible** if cannot be written as a union of proper, Zariski closed subsets.

Similarly, the ideals $\mathcal{I}(V(I))$ and I are not always equal. For $I = \langle F_1, \ldots, F_s \rangle \subset \mathbb{K}[x_1, \ldots, x_n]$, the ideal $J = \langle F_1^{m_1}, \ldots, F_s^{m_s} \rangle$ defines the same variety for any $m_1, \ldots, m_s \in \mathbb{Z}_+$, and hence $\mathcal{I}(V(I)) = \mathcal{I}(V(J))$. This motivates the definition of the *radical* of an ideal.

Definition 2.2.8. For any ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$, the **radical of** I is the ideal given by

$$\sqrt{I} = \{F \in \mathbb{K}[x_1, \ldots, x_n] \,|\, F^m \in I \text{ for some } m \in \mathbb{Z}_+\}.$$

An ideal is said to be **radical** if $\sqrt{I} = I$.

Example 2.2.9. Take $\mathbb{K} = \mathbb{R}$. The variety of $I = \langle x^3 + y^3 - 1, y \rangle$ is given by the single point $V(I) = \{(1, 0)\}$. Geometrically this can be interpreted as the intersection of the x-axis with the cubic defined by $x^3 + y^3 - 1 = 0$. We can also start with $V(I)$ and write the ideal vanishing on the set as $\mathcal{I}(V(I)) = \langle x - 1, y \rangle$. While I is a radical ideal, it is still the case that $\mathcal{I}(V(I)) \neq I$.

However if we take $\mathbb{K} = \mathbb{C}$, then $V(I) = \{(1, 0), (\omega_1, 0), (\omega_2, 0)\}$, where $1, \omega_1, \omega_2$ are the third roots of unity, and $\mathcal{I}(V(I)) = \langle (x - 1)(x - \omega_1)(x - \omega_2), y \rangle = I$.

The above example illustrates how working over the field of complex numbers can be advantageous. As opposed to the real numbers, $\mathbb{C}$ is *algebraically closed*, meaning every non-constant, univariate polynomial $F \in \mathbb{C}[x]$, has a root in $\mathbb{C}$. The theorem below and many other basic results in algebraic geometry are only true over algebraically closed fields such as $\mathbb{C}$ [30].

Hilbert's Nullstellensatz. If $\mathbb{K}$ is an algebraically closed field and I is an ideal of $\mathbb{K}[x_1, \ldots, x_n]$ then $\mathcal{I}(V(I)) = \sqrt{I}$.

Definition 2.2.10. The space of points $[a_0 : a_1 : \ldots : a_n]$, where $a_i \in \mathbb{K}$ for $i = 0, \ldots, n$ and a_i not all zero, under the equivalence relation

$$[a_0 : a_1 : \ldots : a_n] \sim [\lambda a_0 : \lambda a_1 : \ldots : \lambda a_n], \;\; \lambda \neq 0$$

is defined as **projective n-space** and denoted $\mathbb{KP}^n$. When $\mathbb{K}$ is $\mathbb{R}$ or $\mathbb{C}$, we denote this $\mathbb{RP}^n$ and $\mathbb{CP}^n$ respectively.

The space $\mathbb{K}^n$ can be embedded in $\mathbb{KP}^n$ via the map $(a_1, \ldots, a_n) \mapsto [1 : a_1 : \ldots : a_n]$. Thus we can think of $\mathbb{K}^n$ as the *affine points* of $\mathbb{KP}^n$, and the points where $a_0 = 0$ as the *points at infinity*. This distinction is coordinate dependent as we can map $\mathbb{K}^n$ into $\mathbb{KP}^n$ by setting any coordinate $a_i = 1$.

We can similarly define many of the previous objects in $\mathbb{KP}^n$ and recover their affine counterpart by setting $a_0 = 1$.

Definition 2.2.11. The **projective variety** of a collection of homogeneous polynomials $\mathbf{F}_1, \ldots, \mathbf{F}_s \in \mathbb{K}[x_0, x_1, \ldots, x_n]$ is the set of points in $\mathbb{KP}^n$ where $\mathbf{F}_1, \ldots, \mathbf{F}_s$ all vanish and is denoted $V(\mathbf{F}_1, \ldots, \mathbf{F}_s)$.

For an affine variety $V(F_1, \ldots, F_s)$ we can obtain the associated projective variety by *homogenizing* each polynomial F_i.

Definition 2.2.12. The **homogenization** of the polynomial $F \in \mathbb{K}[x_1, \ldots, x_n]$ is the defined as the homogeneous polynomial $\mathbf{F} = x_0^{deg(F)} F\left(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\right) \in \mathbb{K}[x_0, x_1, \ldots, x_n]$. The **dehomogenization with respect to** x_i of the homogeneous polynomial $\mathbf{F} \in \mathbb{K}[x_0, x_1, \ldots, x_n]$ is given by $F = \mathbf{F}(x_0, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n) \in \mathbb{K}[x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n]$.

In this language, $V(F_1, \ldots, F_s)$ is the set of affine points of the projective variety $V(\mathbf{F}_1, \ldots, \mathbf{F}_s)$ where $\mathbf{F}_i$ denotes the homgenization of F_i. This correspondence allows us to seamlessly switch between working over $\mathbb{K}^n$ and $\mathbb{KP}^n$.

Remark 2.2.13. Projective varieties inherit many of the properties of their associated affine variety. For instance we say S is a *Zariski closed* subset of $\mathbb{KP}^n$ if $S \cap U_i$ is Zariski closed for each $i = 0, \ldots, n$, where U_i is the open subset of $\mathbb{KP}^n$ isomorphic to $\mathbb{K}^n$ one obtains by setting $a_i = 1$. Thus a Zariski closed subset of $\mathbb{KP}^n$ is a projective variety.

More generally one can consider open subsets of projective varieties, called *quasi-projective varities*.

Definition 2.2.14. A **quasi-projective variety** is a subset of $\mathbb{KP}^n$ that is open in its Zariski closure.

Note that all affine varieties can be considered quasi-projective varieties, as they are Zariski dense in the associated projective variety.

Remark 2.2.15. Often we will discuss properties that hold outside of a Zariski closed subset of a variety (or $\mathbb{K}^n$). We say that a *generic* point in a Zariski closed set V has a property if there exists a quasi-projective subvariety $U \subset V$ where the property holds.

2.2.1 Rational maps and their images

In this section we will introduce the notion of rational maps between varieties, as well as Gröbner bases, one of the fundamental symbolic computational tools in algebraic geometry, and then discuss how this tool can help us study the image of a rational map. Let $\mathbb{K}(x_1, \ldots, x_n)$ denote the fraction field of $\mathbb{K}[x_1, \ldots, x_n]$ consisting of rational functions on $\mathbb{K}^n$.

Definition 2.2.16. A **rational map** on $\mathbb{K}^n$ is a map $\phi : \mathbb{K}^n \dashrightarrow \mathbb{K}^m$ given by

$$\phi = (\phi_1, \ldots, \phi_m)$$

for some $\phi_1, \ldots, \phi_m \in \mathbb{K}(x_1, \ldots, x_n)$. Two rational maps on $\mathbb{K}^n$ are equivalent if there exists an open subset of $\mathbb{K}^n$ where both maps are defined and agree.

A rational map ϕ on $\mathbb{K}^n$ induces a corresponding rational map $\boldsymbol{\phi} : \mathbb{KP}^n \dashrightarrow \mathbb{KP}^m$ given by a vector of homogeneous polynomials of the same degree $[\boldsymbol{\phi}_0, \boldsymbol{\phi}_1, \ldots, \boldsymbol{\phi}_m]$, where $\boldsymbol{\phi}_0, \boldsymbol{\phi}_1, \ldots, \boldsymbol{\phi}_m \in \mathbb{K}[x_0, x_1, \ldots, x_n]$, and

$$\left(\frac{\boldsymbol{\phi}_1(1, x_1, \ldots, x_n)}{\boldsymbol{\phi}_0(1, x_1, \ldots, x_n)}, \ldots, \frac{\boldsymbol{\phi}_m(1, x_1, \ldots, x_n)}{\boldsymbol{\phi}_0(1, x_1, \ldots, x_n)}\right) = (\phi_1(x_1, \ldots, x_n), \ldots, \phi_m(x_1, \ldots, x_n)) .$$

Thus ϕ and $\boldsymbol{\phi}$ agree on affine points of $\mathbb{KP}^n$ where they are both defined. Note that this representation is not unique as, for any non-zero, homogeneous $\mathbf{H} \in \mathbb{K}[x_0, x_1, \ldots, x_n]$, the vector $\mathbf{H}\boldsymbol{\phi} = [\mathbf{H}\boldsymbol{\phi}_0, \mathbf{H}\boldsymbol{\phi}_1, \ldots, \mathbf{H}\boldsymbol{\phi}_m]$ defines an equivalent rational map on $\mathbb{KP}^n$ when both functions are defined.

Definition 2.2.17. A vector $\boldsymbol{\phi} = [\boldsymbol{\phi}_0, \boldsymbol{\phi}_1, \ldots, \boldsymbol{\phi}_m]$ whose entries $\boldsymbol{\phi}_0, \boldsymbol{\phi}_1, \ldots, \boldsymbol{\phi}_m \in \mathbb{K}[x_0, x_1, \ldots, x_n]$ are homogeneous polynomials of the same degree d is called a **homogeneous vector of degree** d and the notation $\deg(\boldsymbol{\phi}) = d$ is used. The **base locus** of $\boldsymbol{\phi}$ is the set of points at which all its components are zero. It is the projective variety

$$Bl(\boldsymbol{\phi}) = V(\boldsymbol{\phi}_0, \boldsymbol{\phi}_1, \ldots, \boldsymbol{\phi}_m).$$

Note that a polynomial function on a variety $V = V(F_1, \ldots, F_s)$ does not have a unique representation, as for any point $p \in V$ and polynomial $H \in \mathbb{K}[x_1, \ldots, x_n]$, $H(p) = (H + F)(p)$ where $F \in \langle F_1, \ldots, F_s \rangle$.

Definition 2.2.18. Given a variety $V = V(F_1, \ldots, F_s) \subset \mathbb{K}^n$, the **coordinate ring of** V is the quotient ring defined by $k[V] = {}^{\mathbb{K}[x_1, \ldots, x_n]}\!/_{\mathcal{I}(V)}$.

The coordinate ring of a variety defines an equivalence relation on $\mathbb{K}[x_1, \ldots, x_n]$, where two polynomials are equivalent if and only if they define the same function on V. The *fraction field* of $k[V]$, denoted $k(V)$, is known as the ring of rational functions on the variety V.

Definition 2.2.19. For a variety $V = V(F_1, \ldots, F_s) \subset \mathbb{K}^n$, the **ring of rational functions** $\mathbb{K}(V)$ is given by

$$\mathbb{K}(V) = \left\{ \frac{F}{G} \,|\, F, G \in \mathbb{K}[V], G \text{ not a zero divisor} \right\}.$$

The condition that the denominator not be a zero divisor in $\mathbb{K}[V]$ ensures the rational function is defined on a Zariski dense subset of V. Two rational maps ϕ^1 and ϕ^2 define the same map on a variety V, if they are both defined on V and their component functions $\phi^1_1, \ldots, \phi^1_m$ and $\phi^2_1, \ldots, \phi^2_m$ give the same elements in $\mathbb{K}(V)$.

Definition 2.2.20. The rational map $\phi : V \dashrightarrow \mathbb{K}^m$ is **regular** if for each $p \in V \subset \mathbb{K}^n$ there exists $\phi_1, \ldots, \phi_m \in k(x_1, \ldots, x_n)$ such that $\phi(p) = (\phi_1(p), \ldots, \phi_m(p))$.

Remark 2.2.21. Often we will conflate the restriction of a rational map on a variety V, which is an equivalence class of rational functions, with a particular representation $\phi : V \dashrightarrow \mathbb{K}^m$. This distinction can be avoided in many cases as any two representations of the rational map will agree on a *Zariski dense* subset of V. Similarly the images of two different representations will be equivalent up to differences by smaller dimensional subsets; in particular they will have the same Zariski closure.

A rational map on a variety $V = V(F_1, \ldots, F_s)$, given by $\phi : V \dashrightarrow \mathbb{K}^m$, also induces a corresponding rational map on the associated projective variety $\mathbf{V} = V(\mathbf{F}_1, \ldots, \mathbf{F}_s)$ given by any homogeneous vector of degree d, $\boldsymbol{\phi} = [\boldsymbol{\phi}_0, \boldsymbol{\phi}_1, \ldots, \boldsymbol{\phi}_m]$, that defines a *projective extension of* ϕ.

Definition 2.2.22. For any rational map on a variety $\phi : V \dashrightarrow \mathbb{K}^m$, the rational map $\boldsymbol{\phi} : \mathbb{KP}^n \dashrightarrow \mathbb{KP}^m$ given by the homogeneous vector of degree d, $\boldsymbol{\phi} = [\boldsymbol{\phi}_0 : \boldsymbol{\phi}_1 : \ldots : \boldsymbol{\phi}_m]$ is a **projective extension of** ϕ if

$$\phi(1, a_1, \ldots, a_n) = \left(\frac{\phi_1(1, a_1, \ldots, a_n)}{\phi_0(1, a_1, \ldots, a_n)}, \ldots, \frac{\phi_m(1, a_1, \ldots, a_n)}{\phi_0(1, a_1, \ldots, a_n)} \right)$$

and $(1, a_1, \ldots, a_n) \notin Bl(\boldsymbol{\phi})$ for a Zariski dense set of points $(1, a_1, \ldots, a_n) \in V$ where ϕ is defined.

Remark 2.2.23. For any projective extension $\boldsymbol{\phi}$ of the rational map $\phi : V \dashrightarrow \mathbb{K}^m$, the set of affine points of $\overline{\boldsymbol{\phi}(\mathbf{V})}$ is exactly the Zariski-closure of the image of V under ϕ, i.e.

$$\left(\overline{\boldsymbol{\phi}(\mathbf{V})} \cap \{a_0 = 1\}\right) = \overline{\phi(V)}.$$

Note that a polynomial $F \in \mathbb{K}[x_1, \ldots, x_m]$ vanishes on the image of $\phi : V \dashrightarrow \mathbb{K}^m$ if $F(\phi_1, \ldots, \phi_m) = 0$ for all points in V, or equivalently $F(\phi_1, \ldots, \phi_m) = 0$ in $\mathbb{K}(V)$. When the target variety $W \in \mathbb{K}^m$ is clear, we make this explicit by writing $\phi : V \dashrightarrow W$.

Definition 2.2.24. A rational map between (projective) varieties $\phi : V \dashrightarrow W$ is **dominant** if $\overline{\phi(V)} = W$.

For irreducible varieties, rational maps can give a notion of ismorphism between open subsets of the varieties called *birational equivalence*.

Theorem 2.2.25. Let $\phi : V \dashrightarrow W$ be a dominant rational map between (projective) varieties. If V is an irreducible (projective) variety then W is an irreducible (projective) variety.

Definition 2.2.26. A rational map $\phi : V \dashrightarrow W$ between irreducible (projective) varieties is **birational** if there exists a rational map $\psi : W \dashrightarrow V$ such that $\phi \circ \psi$, $\psi \circ \phi$ are identity mappings (where defined), $\phi(V)$ is Zariski dense in W, and $\psi(W)$ is Zariski dense in V. In this case we say that V and W are **birational** or **birationally equivalent**.

The following theorem due to Chevalley [28] again illustrates why working over an algebraically field is advantageous.

Theorem 2.2.27. Let $\mathbb{K}$ be an algebraically closed field. If $\boldsymbol{\phi} : \mathbf{V} \dashrightarrow \mathbf{W}$ is a dominant rational map between projective varieties, then $\boldsymbol{\phi}(\mathbf{V})$ contains an open subset of $\mathbf{W}$.

When simply given a rational map on a variety $\phi : V \dashrightarrow \mathbb{K}^m$, determining the polynomials that vanish on its image (and thereby the image's Zariski closure) is a difficult problem, known as *implicitization*. One can use elimination algorithms to determine these polynomials; the following appears in [30]:

Proposition 2.2.28. Let $\phi : V \dashrightarrow \mathbb{K}^m$ be a rational map on $V = V(F_1, \ldots, F_s)$ given by $\phi = \left(\frac{H_1}{G_1}, \ldots, \frac{H_m}{G_m}\right)$ and $G = \Pi_{i=1}^m G_i$. Then the graph of ϕ is given by the ideal

$$J = \langle G_1 y_1 - H_1, \ldots, G_m y_m - H_m, F_1, \ldots, F_s, zG - 1 \rangle,$$

and $\overline{\phi(V)} = V(J \cap \mathbb{K}[y_1, \ldots, y_m])$.

One can also use elimination to *saturate* an ideal I by a polynomial F, meaning that we remove the component of $V(I)$, corresponding to $V(F)$. This saturation ideal can be found by adding the generator $zF-1$ to I, which removes points corresponding to $V(F)$, and then eliminating z. In particular saturation is important for the algorithms we propose in Appendix A.

Definition 2.2.29. The **saturation ideal of I by F** is given by the ideal

$$(I : F^\infty) = \{G \in I \,|\, G \cdot F^N \in I \text{ for } N \text{ sufficiently large}\}.$$

Proposition 2.2.30. For an ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ and a polynomial $F \in \mathbb{K}[x_1, \ldots, x_n]$,

$$V(I : F^\infty) = \overline{V(I) \backslash V(F)}.$$

See [16] for the above proposition. One of the most powerful tools to eliminate are *Gröbner bases*, which is a particular generating set for the polynomial ideal depending on a chosen *monomial ordering* (for a precise definition see [30]). Gröbner bases were first introduced by Buchberger who gave an algorithm (known as Buchberger's algorithm) to construct a Gröbner basis from any polynomial basis [9].

A Gröbner basis for a polynomial ideal makes it easier to answer certain questions about the ideal and thereby the ideal's associated variety. A polynomial F lies in a polynomial ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ if and only if the Division Algorithm yields 0 when dividing by a Gröbner basis. A Gröbner basis can also help determine the dimension of $V(I)$ and, over an algebraically closed field, the number of points in $V(I)$ when $V(I)$ is zero dimensional. In particular, with an appropriate choice of monomial ordering, $V(J \cap \mathbb{K}[y_1, \ldots, y_m])$ in Proposition 2.2.28 above is generated by $B \cap \mathbb{K}[y_1, \ldots, y_m]$ where $B = \{P_1, \ldots, P_k\}$ is a Gröbner basis for J.

While many of the algorithms involving Gröbner bases are relatively straightforward, in general it can very computationally intensive to find a Gröbner base for a polynomial ideal, especially as the number of variables and the degree of the polynomials grow. For this reason it can be advantageous to study properties of polynomial ideals without computing a Gröbner basis or to instead study a more manageable ideal. For example, in certain cases such as zero dimensional ideals, there exist algorithms that can more efficiently compute a Gröbner basis.

2.2.2 Algebraic curves and intersection multiplicity

We will start by discussing one of the main objects of study in this thesis, plane algebraic curves, and then introduce the idea of *multiplicity* and *intersection multiplicity* in this context before defining it in a more general setting. We will end with one of the most well known theorems in algebraic geometry about curves, Bezout's Theorem.

Definition 2.2.31. A **plane algebraic curve** $X \subset \mathbb{C}^2$ is the curve in the complex plane defined by the zero set over $\mathbb{C}$ of some polynomial $F(x, y) \in \mathbb{C}[x, y]$.

In this section and throughout, X will refer to a planar algebraic curve. The associated projective curve will be denoted $\mathbf{X} = V(\mathbf{F})$, where $\mathbf{F}(x_0, x_1, x_2) \in \mathbb{C}[x_0, x_1, x_2]$ is the homogenization of $F(x, y)$. Later we will restrict our attention to *irreducible* algebraic curves.

Remark 2.2.32. An algebraic curve $X = V(F)$ is irreducible if and only if $F(x, y)$ is irreducible. In this case $F(x, y)$ uniquely defines the curve up to scaling.

The term multiplicity often first appears when discussing univariate polynomials. By the Fundamental Theorem of Algebra, a univariate polynomial $f(x) \in \mathbb{C}[x]$ can be factored as

$$f(x) = (x - a_1)^{r_1}(x - a_2)^{r_2} \dots (x - a_s)^{r_s},$$

where r_i denotes the multiplicity of the root a_i for $i = 1, \dots, s$. This implies that $\frac{d^k}{dx^k}(f)(a_i)$ vanishes for $k < r_i$ and is non-zero for $k = r_i$. Equivalently one can take this as the definition of multiplicity for a univariate polynomial; a value $a \in \mathbb{C}$ has multiplicity r if $\frac{d^k}{dx^k}(f)(a)$ is zero for all $k < r$ and non-zero when $k = r$. Particularly if a is not a root of $f(x)$, then the multiplicity is zero. This definition also generalizes to other smooth, univariate functions.

For algebraic curves we can similarly define the multiplicity at a point in terms of the partials of $F(x, y)$.

Definition 2.2.33. Given an algebraic curve $X = V(F)$, the **multiplicity of X at a point** $p \in \mathbb{C}^2$ is denoted by $m_p(F)$ and is the highest order for which all partial derivatives of $F(x, y)$ of lower order vanish at p, i.e.

$$\frac{d^k}{dx^i dy^j}(F)(p) = 0, \quad i + j = k$$

when $0 \leq k < m_p(F)$ and not when $k = m_p(F)$. If $m_p(F) > 1$ then we say that p is a **singular** point of X and **non-singular** if $m_p(F) = 1$. We say that a curve is **non-singular** if it contains no singular points.

Note that this definition of multiplicity is translation invariant, meaning if $\overline{F}(x, y) = F(x+a, y+b)$ for some fixed $a, b \in \mathbb{C}$ then $\frac{d^k}{dx^i dy^j}\left(\overline{F}\right)(x, y) = \frac{d^k}{dx^i dy^j}(F)(x, y)$. For this reason it is instructive to consider $m_{(0,0)}(F)$; equivalently one can define $m_{(0,0)}(F)$ and extend this definition to any $p \in \mathbb{C}^2$. The following proposition appears in [23]:

Proposition 2.2.34. For an algebraic curve $X = V(F)$ of degree d, let $F = F_m + F_{m+1} + \dots + F_d$, where F_i denotes a homogeneous *form* of degree i. Then $m_{(0,0)}(F) = m$.

When two distinct curves $X = V(F)$ and $Y = V(G)$ intersect, at each point of intersection $p \in X \cap Y$ we can assign a positive integer called the *intersection multiplicity of X and Y at p*. Intuitively, we can think of G as defining a function on X that is zero at each point of intersection, and the intersection multiplicity of Y and X being the multiplicity of the zero of G at p.

Example 2.2.35. Let $X = V(F)$ where $F = \sum_{i,j} a_{ij} x^i y^j$, $a_{ij} \in \mathbb{C}$, and $L = V(\alpha y - \beta x)$, $\alpha, \beta \in \mathbb{C}$, be a line through the origin. We can parameterize the line L by $(x(t), y(t)) = (\alpha t, \beta t)$. Then the restriction of F to L is given by

$$F(\alpha t, \beta t) = a_{00} + (a_{10}\alpha + a_{01}\beta)t + (a_{20}\alpha^2 + a_{11}\alpha\beta + a_{02}\beta^2)t^2 + h(t)$$

where $h(t)$ is a polynomial where the lowest degree in t is ≥ 3. Let the multiplicity of the root $t = 0$ be the intersection multiplicity of X and L at the origin.

From this we can see that the intersection multiplicity is zero if and only if the curve doesn't contain the origin, i.e. $a_{00} \neq 0$. If $a_{00} = 0$ then the intersection multiplicity of L and X is one if and only if $a_{10}\alpha + a_{01}\beta \neq 0$. In this case if the origin is a non-singular point of X, then this condition implies that L is not tangent to X at the origin.

Since $a_{ij} = 0$ if and only if $\frac{d^k}{dx^i dy^j}(F)(0,0) = 0$, it is easy to see that the intersection multiplicity is bounded below by the multiplicity of X at the origin.

More generally we can define the multiplicity of a zero-dimensional ideal at a point, using *local rings*.

Definition 2.2.36. The **local ring of $\mathbb{K}^n$ at p**, denoted $\mathcal{O}_p(\mathbb{K}^n)$, is the set of rational functions on $\mathbb{K}^n$ that are defined at $p \in \mathbb{K}^n$, i.e. $\mathcal{O}_p(\mathbb{K}^n)$ is the subring of $\mathbb{K}(x_1, \ldots, x_n)$ of elements $\frac{P}{Q} \in \mathbb{K}(x_1, \ldots, x_n)$ such that $Q(p) \neq 0$.

Definition 2.2.37. Given a zero-dimensional ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$, the **multiplicity of I at a point** $p \in V(I)$ is given by

$$m_p(I) = \dim_{\mathbb{K}} \left(\mathcal{O}_p(\mathbb{K}^n) \big/ I \cdot \mathcal{O}_p(\mathbb{K}^n) \right),$$

where $I \cdot \mathcal{O}_p(\mathbb{K}^n)$ denotes the ideal generated by I in $\mathcal{O}_p(\mathbb{K}^n)$.

Proposition 2.2.38. If $\mathbb{K}$ is an algebraically closed field and $I \subset \mathbb{K}[x_1, \ldots, x_n]$ is a zero-dimensional ideal, then

$$\sum_{p \in V(I)} m_p(I) = \dim_{\mathbb{K}} \left(\mathbb{K}[x_1, \ldots, x_n] \big/ I \right).$$

See [16] for the above proposition. In the context of curves, this definition might seem unintuitive at first. Similar to Fulton's introduction of this concept in [23] we will start by defining the intersection multiplicity of two curves $X = V(F)$ and $Y = V(G)$ at p in terms of the properties we would want this number to have and then claim that it matches the above definition for $I = \langle F, G \rangle$.

Definition 2.2.39. For two curves $X = V(F)$ and $Y = V(G)$ the **interesection multiplicity of X and Y at p**, denoted $m_p(F, G)$, is a quantity that satisfies the following

1. When X and Y do not share a common component, $m_p(F, G)$ is a nonnegative integer. Otherwise $m_p(F, G) = \infty$.
2. $m_p(F, G) = 0$ if and only if $p \notin X \cap Y$.
3. Let $\overline{F}(x, y) = F(g \cdot (x, y))$ and $\overline{G}(x, y) = G(g \cdot (x, y))$ for some $g \in \mathcal{A}(2)$. Then
$$m_p(F, G) = m_{g \cdot p}(\overline{F}, \overline{G}).$$
4. $m_p(F, G) = m_p(G, F)$.
5. $m_p(F, G) \geq m_p(F)m_p(G)$, with equality occuring if and only if F and G have no tangent lines in common at p.
6. If $F = \Pi_{i=1}^{k} F_i^{r_i}$ and $G = \Pi_{j=1}^{l} G_j^{s_j}$ for some polynomials $F_i^{r_i}, G_j^{s_j} \in \mathbb{C}[x, y]$ where $r_i, s_j \in \mathbb{N}$, then
$$m_p(F, G) = \sum_{i,j} r_i s_j m_p(F_i, G_j).$$
7. $m_p(F, G) = m_p(F, G + HF)$ for any $H \in \mathbb{C}[x, y]$.

Theorem 2.2.40. For any two curves $X = V(F)$ and $Y = V(G)$ and points $p \in \mathbb{C}^2$, there is a unique number $m_p(F, G)$ satisfying conditions (1)-(7) in Definition 2.2.39. Furthermore
$$m_p(F, G) = m_p(\langle F, G \rangle).$$

We can also connect the intersection multiplicity to the initial notion of the multiplicity of the zero at p, for the function defined by restricting one curve to another. To do this we locally parameterize a curve by Taylor series or, more generally, *Laurent series*.

Definition 2.2.41. A **Laurent series** is a power series that includes terms of negative degree which converges for all nonzero t in a neighborhood around $t = 0$, i.e. a series $\alpha(t) = \sum_{i=k}^{\infty} a_i t^i$, for some $k \in \mathbb{Z}$. The **valuation** of α, denoted $\text{val}(\alpha)$, is the smallest power of t with nonzero coefficient.

Theorem 2.2.42. Suppose that $X = V(F)$ is an irreducible curve and $Y = V(G)$ is a curve, which may or may not be irreducible. Then at each nonsingular point $p = (p_1, p_2)$ of X, there exists a parametrization $\alpha(t) = (p_1 + t, p_2 + \sum_{i=1}^{\infty} a_i t^i)$ when $F_y(p) \neq 0$ or $\alpha(t) = (p_1 + \sum_{i=1}^{\infty} a_i t^i, p_2 + t)$ when $F_x(p) \neq 0$ such that

1. $F(\alpha(t)) = 0$ for all $t \in U$, where U is a neighborhood of $t = 0$, and
2. $m_p(F, G) = \text{val}(G(\alpha))$.

Proof. Without loss of generality assume that $F_y(p) \neq 0$. By the implicit function theorem, in a neighborhood of $p = (p_1, p_2)$ in X the curve agrees with the graph $y = f(x)$ for some analytic function f, meaning $F(x, f(x)) = 0$. Thus in a neighborhood $U \subset \mathbb{C}$ of p_1, there exists a power series expansion

$$\sum_{i=1}^{\infty} a_j (x - p_1)^j = f(x)$$

where $a_j = \frac{f^{(j)}(p_2)}{j!}$. Letting $t = x - p_1$ proves (1). For the claim that (2) holds and a more detailed proof of the theorem, see [22]. □

Each method of computing $m_p(F, G)$ for two curves has advantages and drawbacks in different situations. We will make use of both of these to prove our results and to compute these numbers for specific examples. For projective varieties and curves we can also define intersection multiplicity at a point by dehomogenizing to the correct affine chart.

Remark 2.2.43. For a zero-dimensional projective variety defined by the homogeneous polynomial ideal $J \subset \mathbb{K}[x_0, x_1, \ldots, x_n]$ and $\mathbf{p} \in V(J) \subset \mathbb{KP}^n$, the multiplicity of J at $\mathbf{p}$ is given by

$$m_{\mathbf{p}}(J) = m_p(I)$$

where I is the dehomogenization of J with respect to a nonzero coordinate of $\mathbf{p}$. Similarly the intersection multiplicity of a point $\mathbf{p} \in \mathbf{X} \cap \mathbf{Y}$ where $\mathbf{X} = V(\mathbf{F}), \mathbf{Y} = V(\mathbf{G}) \subset \mathbb{CP}^2$ is given by

$$m_{\mathbf{p}}(\mathbf{F}, \mathbf{G}) = m_p(F, G)$$

where F and G are dehomogenized with respect to a nonzero coordinate of $\mathbf{p}$.

With this in hand, we can now state Bezout's theorem, which characterizes the sum of the intersection multiplicities of two curves in terms of their degree [30].

Theorem 2.2.44. Suppose that $\mathbf{X} = V(\mathbf{F})$ and $\mathbf{Y} = V(\mathbf{G})$ are two projective curves in $\mathbb{CP}^2$ of degree n and m respectively with no common factors. Then

$$\sum_{\mathbf{p} \in V(\mathbf{F}) \cap V(\mathbf{G})} m_{\mathbf{p}}(\mathbf{F}, \mathbf{G}) = m \cdot n.$$

2.2.3 Image of an algebraic curve under a rational map

In this section, an irreducible, projective curve $\mathbf{X} = V(\mathbf{F})$ refers to a curve in $\mathbb{CP}^2$. We discuss the special case of the image of an irreducible, projective curve under the rational map $\boldsymbol{\phi} : \mathbb{CP}^2 \dashrightarrow \mathbb{CP}^2$ defined by a vector of homogeneous polynomials $\boldsymbol{\phi} = [\boldsymbol{\phi}_0, \boldsymbol{\phi}_1, \boldsymbol{\phi}_2]$. In particular, we show that one can find the degree, as well as the highest degree in each variable, of the minimal polynomial vanishing on $\boldsymbol{\phi}(\mathbf{X})$. To do this we use a well-known result due to Bertini as it appears in [50]:

Bertini's Theorem on Generic Smoothness. Let $U \in \mathbb{CP}^n$ be a nonsingular, quasi-projective variety and $\boldsymbol{\phi} : U \to Y$ be a dominant, regular rational map between U and a quasi-projective variety $Y \subset \mathbb{CP}^m$. Then there exists a dense open subset $V \subset Y$ such that the fiber $\boldsymbol{\phi}^{-1}(y)$ is nonsingular for every $y \in V$.

More specifically, a particular case is invoked. For a homogeneous vector of polynomials $\boldsymbol{\phi} = [\boldsymbol{\phi}_0, \boldsymbol{\phi}_1, \ldots \boldsymbol{\phi}_m]$ denote the polynomial defined by $\mathbf{a} = [a_0 : a_1 : \ldots : a_m]$ as

$$\boldsymbol{\phi}^*_{\mathbf{a}} = a_0\boldsymbol{\phi}_0 + a_1\boldsymbol{\phi}_1 + \ldots + a_m\boldsymbol{\phi}_m.$$

We show that the following corollary is a direct consequence of Bertini's theorem.

Corollary 2.2.45. Let $\mathbf{X} = V(\mathbf{F}) \subset \mathbb{C}^2$ be an irreducible projective variety and $\boldsymbol{\phi} = [\boldsymbol{\phi}_0, \boldsymbol{\phi}_1, \ldots, \boldsymbol{\phi}_m]$ be a homogeneous vector of polynomials in $\mathbb{C}[x_0, x_1, x_2]$, $m \geq 1$. Then for a generic choice of $\mathbf{a} = [a_0 : a_1 : \ldots : a_m] \in \mathbb{CP}^m$, $\boldsymbol{\phi}^*_{\mathbf{a}}$ intersects $\mathbf{X}$ transversely outside of the base locus of $\boldsymbol{\phi}$, i.e.

$$m_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi}^*_{\mathbf{a}}) = 1$$

for all $\mathbf{p} \in V(\mathbf{F}) \cap (V(\boldsymbol{\phi}^*_{\mathbf{a}}) \backslash Bl(\boldsymbol{\phi}))$.

Proof. Consider the quasi-projective variety

$$\mathbf{V} \;=\; \left\{(\mathbf{p}, \mathbf{a}) \in \mathbb{CP}^2 \times \mathbb{CP}^m \,|\, \mathbf{p} \in V(\mathbf{F}, \boldsymbol{\phi}^*_{\mathbf{a}}),\, \mathbf{p} \notin Bl(\boldsymbol{\phi}) \cup V(\mathbf{F})_{sing}\right\}$$

where $V(\mathbf{F})_{sing}$ denotes the variety $V(\frac{\partial \mathbf{F}}{\partial x_0}, \frac{\partial \mathbf{F}}{\partial x_1}, \frac{\partial \mathbf{F}}{\partial x_2})$. A point $(\mathbf{p}, \mathbf{a}) \in \mathbf{V}$ is a singular point of $\mathbf{V}$ if and only if the Jacobian matrix

$$\begin{bmatrix} \frac{\partial F}{\partial x_0} & \frac{\partial F}{\partial x_1} & \frac{\partial F}{\partial x_2} & 0 & \dots & 0 \\ \frac{\partial \boldsymbol{\phi}^*_{\mathbf{a}}}{\partial x_0} & \frac{\partial \boldsymbol{\phi}^*_{\mathbf{a}}}{\partial x_1} & \frac{\partial \boldsymbol{\phi}^*_{\mathbf{a}}}{\partial x_2} & \boldsymbol{\phi}_0 & \dots & \boldsymbol{\phi}_m \end{bmatrix}$$

drops rank. Thus the removal of $V(\mathbf{F})_{sing}$ and $Bl(\boldsymbol{\phi})$ ensures that $\mathbf{V}$ is nonsingular. The projection $\pi : \mathbf{V} \to \mathbb{CP}^m$ defined by $\pi(\mathbf{p}, \mathbf{a}) = \mathbf{a}$ is a dominant, regular rational map and Bertini's Theorem says there exists an open subset $U \subset \mathbb{CP}^m$ where a generic fiber of this map is nonsingular. The hypotheses of Bertini's Theorem further imply that the induced map on the tangent spaces $d_{(\mathbf{p},\mathbf{a})}\pi : T_{\mathbf{V},(\mathbf{p},\mathbf{a})} \to T_{\mathbb{CP}^m,\mathbf{a}}$ which takes $(\mathbf{q}, \mathbf{b}) \in T_{\mathbf{V},(\mathbf{p},\mathbf{a})}$ to $\mathbf{b} \in T_{\mathbb{CP}^m,\mathbf{a}}$ is surjective for each $(\mathbf{p}, \mathbf{a}) \in \boldsymbol{\pi}^{-1}(U)$ [50, Ch. 2, Sec. 6]. The tangent space $T_{\mathbf{V},(\mathbf{p},\mathbf{a})}$ is given by

$$T_{\mathbf{V},(\mathbf{p},\mathbf{a})} = \{(\mathbf{q}, \mathbf{b}) \in \mathbb{CP}^2 \times \mathbb{CP}^m \mid \nabla \mathbf{F}(\mathbf{p}) \cdot \mathbf{q} = 0,\ \nabla \boldsymbol{\phi}^*_{\mathbf{a}}(\mathbf{p}) \cdot \mathbf{q} + \boldsymbol{\phi}(\mathbf{p}) \cdot \mathbf{b} = 0\},$$

where ∇ denotes the gradient of a polynomial and $\cdot$ indicates dot product. If $\mathbf{p}$ is a singular point of $\boldsymbol{\phi}^*_a$ or if $\nabla \mathbf{F}(\mathbf{p})$ and $\nabla \boldsymbol{\phi}^*_{\mathbf{a}}(\mathbf{p})$ are linearly dependent, then for any $(\mathbf{q}, \mathbf{b}) \in T_{\mathbf{V},(\mathbf{p},\mathbf{a})}$, $\boldsymbol{\phi}(\mathbf{p}) \cdot \mathbf{b} = 0$, implying the map $d_{(\mathbf{p},\mathbf{a})}\pi$ is not surjective. Thus $m_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi}^*_{\mathbf{a}}) = 1$ whenever $\mathbf{a} \in U$ and $(\mathbf{p}, \mathbf{a}) \in \mathbf{V}$.

We can further assume that for each $\mathbf{a} \in U$, $V(\mathbf{F}) \cap (V(\boldsymbol{\phi}^*_{\mathbf{a}}) \backslash Bl(\boldsymbol{\phi}))$ contains no singular points of $\mathbf{X}$ since this is a generic condition on $\mathbb{CP}^m$. Therefore for $\mathbf{a} \in U$, each point $\mathbf{p} \in V(\mathbf{F}) \cap (V(\boldsymbol{\phi}^*_{\mathbf{a}}) \backslash Bl(\boldsymbol{\phi}))$ is an element of $\mathbf{V}$, proving the theorem. □

The Corollary above characterizes $m_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi}^*_{\mathbf{a}})$ for points outside of $Bl(\boldsymbol{\phi})$, for a generic choice of a parameter $a \in \mathbb{CP}^m$. When $\mathbf{X} = V(\mathbf{F})$ is a curve, we can also say something about $m_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi}^*_{\mathbf{a}})$ when $\mathbf{p} \in Bl(\boldsymbol{\phi})$.

Lemma 2.2.46. Let $\mathbf{X} = V(\mathbf{F})$ be an irreducible algebraic curve and $\boldsymbol{\phi} = [\boldsymbol{\phi}_0, \boldsymbol{\phi}_1, \dots, \boldsymbol{\phi}_m]$ be a homogeneous vector defined on $\mathbf{X}$ where $m \geq 1$. For $\mathbf{p} \in \mathbf{X} \cap Bl(\boldsymbol{\phi})$, the minimum of $m_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi}^*_{\mathbf{a}})$ over all $\mathbf{a} = [a_0 : a_1 : \dots : a_m] \in \mathbb{CP}^m$ is achieved generically.

Proof. Suppose that $\mathbf{p}$ is a non-singular point of $\mathbf{X}$. By Theorem 2.2.42 there exists a local parameterization of $\mathbf{X}$ about $\mathbf{p}$, denoted α where $m_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi}^*_{\mathbf{a}}) = \text{val}(\boldsymbol{\phi}^*_{\mathbf{a}}(\alpha))$. The expression $\boldsymbol{\phi}^*_{\mathbf{a}}(\alpha)$ is a power series in t, which each coefficient of t a linear form in $\mathbb{C}[a_0, a_1, \dots, a_m]$. Thus the condition that $m_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi}^*_{\mathbf{a}}) \geq n$ for any $n \in \mathbb{Z}_+$ is a linear condition on $\mathbf{a} \in \mathbb{CP}^m$.

Now suppose $\mathbf{p}$ is a singular point of $\mathbf{X}$. Consider a non-singular model $\mathcal{Y}$ of the curve with birational map $\boldsymbol{\psi} : \mathcal{Y} \to \mathbf{X}$ (see [23, Ch. 7]). Let $\boldsymbol{\psi}^*_{\mathbf{a}}$ denote the pullback of $\boldsymbol{\phi}^*_{\mathbf{a}}$ under $\boldsymbol{\psi}$ given by $\boldsymbol{\phi}^*_a(\boldsymbol{\psi}_0, \boldsymbol{\psi}_1, \boldsymbol{\psi}_2)$. Then $m_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi}^*_{\mathbf{a}})$ equals $\sum_{\mathbf{q} \in \boldsymbol{\psi}^{-1}(\mathbf{p})} m_{\mathbf{q}}(\mathcal{Y}, \boldsymbol{\psi}^*_{\mathbf{a}})$ [23, Ch. 7, Prop. 2]. As in the non-singular case, one can locally parameterize the curve $\mathcal{Y}$ to determine the intersection multiplicity of $\mathcal{Y}$ and $\boldsymbol{\psi}^*_{\mathbf{a}}$ at $\mathbf{q}$. This reduces to the non-singular case. □

Remark 2.2.47. The minimum multiplicity in Lemma 2.2.46 will reappear frequently and we denote it by

$$\text{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi}) = \min_{\mathbf{a} \in \mathbb{CP}^m} m_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi}^*_{\mathbf{a}}).$$

The following bounds can be useful for computing this intersection multiplicity:

Proposition 2.2.48. Let $\mathbf{X} = V(\mathbf{F})$ be an irreducible algebraic curve and $\boldsymbol{\phi} = [\phi_0, \phi_1, \ldots, \phi_m]$ be a homogeneous vector defined on $\mathbf{X}$ where $m \geq 1$. For $\mathbf{p} \in \mathbf{X} \cap Bl(\boldsymbol{\phi})$ and any $\mathbf{a} = [a_0 : a_1 : \ldots : a_m] \in \mathbb{CP}^m$,

$$m_{\mathbf{p}}(\langle \mathbf{F}, \phi_0, \phi_1, \ldots, \phi_m \rangle) \leq \text{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi}) \leq m_{\mathbf{p}}(\mathbf{F}, \phi^*_{\mathbf{a}}),$$

where the right inequality is tight for generic $\mathbf{a} \in \mathbb{CP}^m$.

Proof. For the first inequality, note that for any $\mathbf{a} \in \mathbb{CP}^m$, $\boldsymbol{\phi}^*_{\mathbf{a}} = a_0\phi_0 + a_1\phi_1 + \ldots + a_m\phi_m$ belongs to the ideal $\langle \phi_0, \phi_1, \ldots, \phi_m \rangle$. By definition, larger ideals have smaller multiplicities. More precisely, for homogeneous ideals $I \subset J \subset \mathbb{C}[x_0, x_1, x_2]$ and a point $\mathbf{p} \in \mathbb{CP}^2$, we have that $m_{\mathbf{p}}(I) \geq m_{\mathbf{p}}(J)$. Therefore for every point $\mathbf{p} \in \mathbb{CP}^2$, $m_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi}^*\mathbf{L}) \geq m_{\mathbf{p}}(\langle \mathbf{F}, \phi_0, \phi_1, \ldots, \phi_m \rangle)$. The inequality then follows from a generic choice of $\mathbf{a} \in \mathbb{CP}^2$ and Remark 2.2.47.

The second inequality follows directly from the definition of $\text{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi})$, and tightness follows from Lemma 2.2.46. □

One can see, by Theorem 2.2.25 and Chevalley's Theorem, that the image of an irreducible algebraic curve $\mathbf{X} = V(\mathbf{F})$ under the rational map defined by $\boldsymbol{\phi} = [\phi_0, \phi_1, \ldots, \phi_m]$ is all but finitely many points of another irreducible algebraic curve. By Bezout's Theorem the number of intersection points of a generic line with this image will be the curve's degree.

Let the line in the image space defined by $\mathbf{a}$ be given by $\mathbf{L_a} = a_0y_0 + a_1y_1 + a_2y_2$. Then the *pullback* of this line under the rational map defined by $\boldsymbol{\phi}$ is given by $\boldsymbol{\phi}^*_{\mathbf{a}}$. We can deduce much information from $\boldsymbol{\phi}^*_{\mathbf{a}}$ about the irreducible polynomial vanishing on $\boldsymbol{\phi}(\mathbf{X})$.

Remark 2.2.49. For an irreducible algebraic curve $\mathbf{X}$ and a homogeneous vector $\boldsymbol{\phi} = [\phi_0, \phi_1, \phi_2]$, we say that $\boldsymbol{\phi}$ is *defined on* $\boldsymbol{X}$ if $Bl(\boldsymbol{\phi})$ doesn't contain $\mathbf{X}$, i.e. $Bl(\boldsymbol{\phi}) \cap \mathbf{X}$ consists of finitely many points. Furthermore we say that $\boldsymbol{\phi}$ is *non-constant on* $\boldsymbol{X}$ if the induced rational map $\boldsymbol{\phi} : \mathbb{CP}^2 \dashrightarrow \mathbb{CP}^2$ is not constant when restricted to $\mathbf{X}$.

Lemma 2.2.50. Let $\mathbf{X} = V(\mathbf{F})$ be an irreducible algebraic curve and $\boldsymbol{\phi} = [\phi_0, \phi_1, \phi_2]$ be a homogeneous vector defined and non-constant on $\mathbf{X}$. For a generic linear form $\mathbf{L_a} = a_0y_0 + a_1y_1 + a_2y_2 \in \mathbb{C}[y_0, y_1, y_2]$,

(a) $V(\boldsymbol{\phi}^*_{\mathbf{a}}) = \boldsymbol{\phi}^{-1}(V(\mathbf{L_a})) \cup Bl(\boldsymbol{\phi})$

(b) $\mathbf{F}$ and $\boldsymbol{\phi}^*_{\mathbf{a}}$ have no common factors, and

(c) if $\mathbf{p} \in V(\mathbf{F}) \cap (V(\boldsymbol{\phi}^*_{\mathbf{a}}) \backslash Bl(\boldsymbol{\phi}))$ then $m_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi}^*_{\mathbf{a}}) = 1$.

Proof. (a) If $\mathbf{p} \notin Bl(\boldsymbol{\phi})$, then $\boldsymbol{\phi}$ is defined at $\mathbf{p}$. Then $\boldsymbol{\phi}(\mathbf{p})$ belongs to $V(\mathbf{L}_{\mathbf{a}})$ if and only if $\mathbf{p}$ belongs to $V(\boldsymbol{\phi}^*_{\mathbf{a}})$. If $\mathbf{p}$ belongs to $Bl(\boldsymbol{\phi})$, then it clearly also belongs to $V(\boldsymbol{\phi}^*_{\mathbf{a}}$.

(b) Since $\mathbf{F}$ is irreducible, $\boldsymbol{\phi}^*_{\mathbf{a}}$ and $\mathbf{F}$ have a common factor if and only if $\mathbf{F}$ divides $\boldsymbol{\phi}^*_{\mathbf{a}}$. The set of $\mathbf{a} \in \mathbb{CP}^2$ for which $\mathbf{F}$ divides $\boldsymbol{\phi}^*_{\mathbf{a}}$ is Zariski-closed in $\mathbb{CP}^2$ (When $\deg(F) \leq \deg(\boldsymbol{\phi})$, consider the intersection of the subspaces $F \cdot \mathbb{C}[x_0, x_1, x_2]_{\deg(\boldsymbol{\phi})-\deg(F)}$ and $\boldsymbol{\phi}^*_{\mathbf{a}}$ in $\mathbb{C}[x_0, x_1, x_2]_{\deg(\boldsymbol{\phi})}$).

Since $\boldsymbol{\phi}$ is defined on $\mathbf{F}$, there is some $\boldsymbol{\phi}_j$ not divisible by $\mathbf{F}$, and hence this set is not all of $\mathbb{CP}^2$. Therefore there is a nonempty Zariski-open set of $\mathbf{a} \in \mathbb{CP}^2$ for which $\mathbf{F}$ and $\boldsymbol{\phi}^*_{\mathbf{a}}$ have no common factors.

(c)This follows from Corollary 2.2.45.

□

Lemma 2.2.51. Let $\mathbf{X} = V(\mathbf{F})$ be an irreducible algebraic curve and $\boldsymbol{\phi} = [\boldsymbol{\phi}_0, \boldsymbol{\phi}_1, \boldsymbol{\phi}_2]$ be a homogeneous vector defined and non-constant on $\mathbf{X}$. Denote $\boldsymbol{\phi}^0 = [\boldsymbol{\phi}_1, \boldsymbol{\phi}_2]$, $\mathbf{p}^0 = [1:0:0]$, and the linear form $\mathbf{L}^0_{\mathbf{b}} = b_1 y_1 + b_2 y_2$ where $b \in \mathbb{CP}^1$, and define $\boldsymbol{\phi}^i, \mathbf{p}^i$, and $\mathbf{L}^i_{\mathbf{b}}$ similarly for $i = 1, 2$. Then for a generic choice of $\mathbf{b}$ the following hold for $i = 0, 1, 2$:

(a) $V((\boldsymbol{\phi}^i)^*_{\mathbf{b}}) = \boldsymbol{\phi}^{-1}\left(V(\mathbf{L}^i_{\mathbf{b}}) \backslash \mathbf{p}^i\right) \cup Bl(\boldsymbol{\phi}^i)$

(b) $\mathbf{F}$ and $\boldsymbol{\phi}^*_{\mathbf{b}}$ have no common factors, and

(c) if $\mathbf{p} \in V(\mathbf{F}) \cap \left(V((\boldsymbol{\phi}^i)^*_{\mathbf{b}}) \backslash Bl(\boldsymbol{\phi}^i)\right)$ then $m_{\mathbf{p}}(\mathbf{F}, (\boldsymbol{\phi}^i)^*_{\mathbf{b}}) = 1$.

Proof. (a) By the proof of Lemma 2.2.50(a), $\mathbf{q} \in V((\boldsymbol{\phi}^i)^*_{\mathbf{b}})$ if and only if either $\mathbf{q} \in \boldsymbol{\phi}^{-1}(V(\mathbf{L}^i_{\mathbf{b}}))$ or $\mathbf{q} \in Bl(\boldsymbol{\phi})$. Along with the fact that $Bl(\boldsymbol{\phi}^i) = Bl(\boldsymbol{\phi}) \cup \boldsymbol{\phi}^{-1}(\mathbf{p}^i)$, this proves the equality in (a).

(b) Since $\boldsymbol{\phi}$ is not constant on $\mathbf{X}$, no pair of polynomials in $\boldsymbol{\phi}$ can simultaneously contain $\mathbf{F}$ as a factor. The rest of the proof follows similarly as in Lemma 2.2.50(b).

(c) This follows from Corollary 2.2.45.

□

When $\boldsymbol{\phi} = [\boldsymbol{\phi}_0, \boldsymbol{\phi}_1, \boldsymbol{\phi}_2]$ defines a generically $n:1$ map on a curve $\mathbf{X}$, we can translate degree counts in the image space to degree and multiplicity counts in the domain space. The following results show the relationship between the degree of $\overline{\boldsymbol{\phi}(\mathbf{X})}$ and the intersection of $\mathbf{X}$ with the pullback of a line under $\boldsymbol{\phi}$.

Theorem 2.2.52. Let $\mathbf{X} = V(\mathbf{F})$ be an irreducible algebraic curve and $\boldsymbol{\phi} = [\phi_0, \phi_1, \phi_2]$ be a homogeneous vector defined and non-constant on $\mathbf{X}$ such that the induced rational map $\boldsymbol{\phi} : \mathbb{CP}^2 \dashrightarrow \mathbb{CP}^2$ is generically $n:1$ on $\mathbf{X}$. Let $\mathbf{P} \in \mathbb{C}[y_0, y_1, y_2]$ denote the minimal polynomial vanishing on the image $\boldsymbol{\phi}(\mathbf{X})$. Then

$$n \cdot \deg(\mathbf{P}) = \deg(\mathbf{F}) \cdot \deg(\boldsymbol{\phi}) - \sum_{p \in Bl(\boldsymbol{\phi})} \text{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi}). \tag{2.6}$$

Proof. For a generic linear form $\mathbf{L_a} = a_0 y_0 + a_1 y_1 + a_2 y_2 \in \mathbb{C}[y_0, y_1, y_2]$, Bezout's Theorem and Lemma 2.2.50(a) give that

$$\deg(\mathbf{F}) \cdot \deg(\boldsymbol{\phi}^*_{\mathbf{a}}) = \sum_{\mathbf{p}} m_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi}^*_{\mathbf{a}}) = \sum_{\mathbf{p} \in \boldsymbol{\phi}^{-1}(V(\mathbf{L_a}))} m_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi}^*_{\mathbf{a}}) + \sum_{\mathbf{p} \in Bl(\boldsymbol{\phi})} m_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi}^*_{\mathbf{a}}).$$

By the genericity of the choice of $\mathbf{L_a}$ and Lemma 2.2.46, for every $\mathbf{p}$, $m_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi}^*_{\mathbf{a}})$ equals $\text{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi})$.

Genericity also ensures that $\boldsymbol{\phi}^*_{\mathbf{a}}$ is nonzero and its degree equals $\deg(\boldsymbol{\phi})$. By Lemma 2.2.50(c), for each point $\mathbf{p} \in V(\mathbf{F}) \cap \boldsymbol{\phi}^{-1}(V(\mathbf{L_a}))$, the intersection multiplicity $m_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi}^*_{\mathbf{a}})$ equals one. Since $\boldsymbol{\phi}$ is generically $n:1$, there are at most finitely many points $\mathbf{p} \in V(\mathbf{F})$ for which $|\boldsymbol{\phi}^{-1}(\boldsymbol{\phi}(\mathbf{p})) \cap V(\mathbf{F})| \neq n$, meaning that the generic line $V(\mathbf{L_a})$ will not contain the image $\boldsymbol{\phi}(\mathbf{p})$ of any of these points. Therefore for every point $\mathbf{p} \in \boldsymbol{\phi}^{-1}(V(\mathbf{L_a})) \cap V(\mathbf{F})$, there are exactly n points of $V(\mathbf{F})$ in the set $\boldsymbol{\phi}^{-1}(\boldsymbol{\phi}(\mathbf{p}))$. Putting this all together gives that

$$\sum_{\mathbf{p} \in \boldsymbol{\phi}^{-1}(V(\mathbf{L_a}))} m_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi}^*_{\mathbf{a}}) \quad = \quad |V(\mathbf{F}) \cap \boldsymbol{\phi}^{-1}(V(\mathbf{L_a}))| \quad = \quad n \cdot |\boldsymbol{\phi}(V(\mathbf{F})) \cap V(\mathbf{L_a})|.$$

By Chevalley's Theorem, the image $\boldsymbol{\phi}(V(\mathbf{F}))$ is all but finitely many points of its Zariski closure $V(\mathbf{P})$. The genericity of $\mathbf{L_a}$ ensures that every point in $V(\mathbf{L_a}) \cap V(\mathbf{P})$ belongs to $V(\mathbf{L}) \cap \boldsymbol{\phi}(V(\mathbf{F}))$ and that the number of these points equals $\deg(\mathbf{P})$. This proves equality in (2.6). □

For an irreducible, homogeneous polynomial $\mathbf{P} \in \mathbb{K}[x_0, x_1, \ldots, x_n]$ denote the highest degree of x_i appearing in $\mathbf{P}$ as $\deg_{x_i}(\mathbf{P})$.

Theorem 2.2.53. Let $\mathbf{X} = V(\mathbf{F})$ be an irreducible algebraic curve and $\boldsymbol{\phi} = [\phi_0, \phi_1, \phi_2]$ be a homogeneous vector defined and non-constant on $\mathbf{X}$ such that the induced rational map $\boldsymbol{\phi} : \mathbb{CP}^2 \dashrightarrow \mathbb{CP}^2$ is generically $n:1$ on $\mathbf{X}$. Let $\mathbf{P} \in \mathbb{C}[y_0, y_1, y_2]$ denote the minimal polynomial vanishing on the image $\boldsymbol{\phi}(\mathbf{X})$. Denote $\boldsymbol{\phi}^0 = [\phi_1, \phi_2]$ and define $\boldsymbol{\phi}^1, \boldsymbol{\phi}^2$ similarly. Then for $i = 0, 1, 2$

$$n \cdot \deg_{y_i}(\mathbf{P}) = \deg(\mathbf{F}) \cdot \deg(\boldsymbol{\phi}) - \sum_{p \in Bl(\boldsymbol{\phi}^i)} \text{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi}^i). \tag{2.7}$$

Proof. For any projective curve given by $V(\mathbf{P})$ for $\mathbf{P} \in \mathbb{C}[y_0, y_1, y_2]$, the highest degree of y_i is given by $\deg_{y_i}(\mathbf{P}) = \deg(\mathbf{P}) - m_{\mathbf{p}^i}(\mathbf{P})$ (see Proposition 2.2.34). By Bezout's Theorem and Corollary 2.2.45, for a generic choice of $\mathbf{b} \in \mathbb{CP}^1$,

$$\begin{aligned} \deg(\mathbf{P}) &= m_{\mathbf{p}^i}(\mathbf{P}) + |V(\mathbf{P}) \cap \left(V(\mathbf{L}^i_{\mathbf{b}})\backslash \mathbf{p}^i\right)| \\ \deg_{y_i}(\mathbf{P}) &= |V(\mathbf{P}) \cap \left(V(\mathbf{L}^i_{\mathbf{b}})\backslash \mathbf{p}^i\right)|. \end{aligned}$$

The genericity of $\mathbf{L_b}$ and Chevalley's Theorem also ensures that each point in $V(\mathbf{P}) \cap \left(V(\mathbf{L}^i_{\mathbf{b}})\backslash \mathbf{p}^i\right)$ lies in $\boldsymbol{\phi}(V(\mathbf{F}))$ and has exactly n pre-images. Thus

$$|V(\mathbf{F}) \cap \boldsymbol{\phi}^{-1}\left(V(\mathbf{L}^i_{\mathbf{b}})\backslash \mathbf{p}^i\right)| = n \cdot |V(\mathbf{P}) \cap \left(V(\mathbf{L}^i_{\mathbf{b}})\backslash \mathbf{p}^i\right)| = n \cdot \deg_{y_i}(\mathbf{P}). \tag{2.8}$$

Similarly as in the proof of Theorem 2.2.52 and by Lemma 2.2.51,

$$\begin{aligned} \deg(\mathbf{F}) \cdot \deg((\boldsymbol{\phi}^i)^*_{\mathbf{b}}) &= \deg(\mathbf{F}) \cdot \deg(\boldsymbol{\phi}) \\ &= \sum_{\mathbf{p}} m_{\mathbf{p}}(\mathbf{F}, (\boldsymbol{\phi}^i)^*_{\mathbf{b}}) \\ &= \sum_{\mathbf{p} \in \boldsymbol{\phi}^{-1}\left(V(\mathbf{L}^i_{\mathbf{b}})\backslash \mathbf{p}^i\right)} m_{\mathbf{p}}(\mathbf{F}, (\boldsymbol{\phi}^i)^*_{\mathbf{b}}) + \sum_{\mathbf{p} \in Bl(\boldsymbol{\phi}^i)} m_{\mathbf{p}}(\mathbf{F}, (\boldsymbol{\phi}^i)^*_{\mathbf{b}}) \\ &= |V(\mathbf{F}) \cap \boldsymbol{\phi}^{-1}\left(V(\mathbf{L}^i_{\mathbf{b}})\backslash \mathbf{p}^i\right)| + \sum_{\mathbf{p} \in Bl(\boldsymbol{\phi}^i)} \mathrm{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi}^i). \end{aligned}$$

This and (2.8) prove the equality in (2.7). □

While the previous theorems give an explicit formula for the degree of $\overline{\boldsymbol{\phi}(X)}$ and its highest degree in each variable, for any particular choice of $\mathbf{a} = [a_0 : a_1 : a_2]$, there is no guarantee that we've chosen generically. However, using Proposition 2.2.48 we can compute bounds for these quantities. For further discussion of how this can be implemented in symbolic computation software see Appendix A.

2.3 Actions and invariants of algebraic groups

In Section 2.1 we introduced groups, invariants, and the equivalence problem for curves in the most general context, before restricting attention to smooth curves. In doing so, we also assumed that the group had a smooth structure and the map defining the group action was smooth. Similarly when we consider the equivalence problem for algebraic curves, we will require that G be an *algebraic group* acting *rationally*.

Definition 2.3.1. A group G is an **algebraic group** if G can be expressed as an algebraic variety, and the maps defining group multiplication and inverse are regular maps.

Definition 2.3.2. The action of an algebraic group G on an affine or projective variety $\mathcal{Y}$ is **rational** if the map defining the group action (see Definition 2.1.1) given by $\Phi : G \times \mathcal{Y} \dashrightarrow \mathcal{Y}$ is a rational map. The action is **regular** if Φ is a regular map.

Example 2.3.3. The general linear group of invertible $n \times n$ matrices over a field $\mathbb{K}$, denoted $\mathcal{GL}(n, \mathbb{K})$, is an algebraic group. The set $\mathcal{GL}(n, \mathbb{K})$ can be viewed as an algebraic variety in $\mathbb{K}^{n^2+1}$ defined by

$$\{(X, t) \in \mathbb{K}^{n^2+1} \mid \det(X) \cdot t - 1 = 0,\ X \in \mathcal{GL}(n, \mathbb{K})\}.$$

The natural action of $\mathcal{GL}(n, \mathbb{K})$ on $\mathbb{KP}^n$ is given by $\Phi(X, \mathbf{p}) = X \cdot [x_0 : x_1 : \ldots : x_n]^T$ for $X \in \mathcal{GL}(n, \mathbb{K})$ and $\mathbf{p} \in \mathbb{KP}^n$. This action is regular and induces a rational action of $\mathcal{GL}(n, \mathbb{K})$ on $\mathbb{K}^{n-1}$ given by the corresponding rational map of Φ on $\mathbb{K}^{n-1}$.

Remark 2.3.4. The group $\mathcal{SO}(2, \mathbb{R})$ acting on $\mathbb{R}^2$ in Example 2.1.12 is another example of an algebraic group acting rationally on $\mathbb{R}^2$. It can be viewed as the subset of $\mathcal{GL}(3, \mathbb{R})$

$$\mathcal{SO}(2, \mathbb{R}) = \left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & c & s \\ 0 & -s & c \end{bmatrix} \in \mathcal{GL}(3, \mathbb{R}) \;\middle|\; c, s \in \mathbb{R},\ c^2 + s^2 - 1 = 0\} \right\},$$

with the same action as defined in Example 2.3.3. Similarly one can view $\mathcal{SE}(2, \mathbb{R})$ and $\mathcal{SA}(2, \mathbb{R})$ from Examples 2.1.13 and 2.1.14 as algebraic groups acting rationally on $\mathbb{R}^2$.

Many results on algebraic groups are only true over an algebraic closed field of characteristic zero, and thus we assume for the remainder of Section 2.3 that the ground field is $\mathbb{C}$. Unless otherwise stated, we additionally assume that "action" refers to a rational action and that "open" and "closed" refer to the Zariski topology. See [54] for more details:

Proposition 2.3.5. For an algebraic group G acting on an affine or projective variety $\mathcal{Y}$ the following hold:

1. For any $p \in \mathcal{Y}$, the stabilizer G_p is a closed algebraic subgroup of G.
2. The orbit Gp is a quasi-projective variety and

$$\dim Gp = \dim G - \dim G_p.$$

3. If $\mathcal{Y}$ is irreducible then the set of all points whose orbit dimension is less than maximal (equivalently the dimension of the stabilizer group is greater than minimum) lies in a closed, proper subset of $\mathcal{Y}$.

4. Finally, if G is irreducible, then for all $p \in \mathcal{Y}$ the closure of the orbit $\overline{Gp}$ is irreducible.

For actions of algebraic groups on a variety $\mathcal{Y}$ we consider rational functions on $\mathcal{Y}$ that are invariant under G.

Definition 2.3.6. A rational function $K \in \mathbb{C}(\mathcal{Y})$ on $\mathcal{Y}$ is **G-invariant** if $K(g \cdot p) = K(p)$, whenever both sides are defined. The set of all G-invariant rational function on $\mathcal{Y}$ is denoted $\mathbb{C}(\mathcal{Y})^G$ and is a subfield of $\mathbb{C}(\mathcal{Y})$.

Definition 2.3.7. A subset $\mathcal{I} \subset \mathbb{C}(\mathcal{Y})^G$ is called **separating** if there exists a nonempty open subset $W \subset \mathcal{Y}$ such that $\mathcal{I}$ is separating on W (see Definition 2.1.10). The set W is called a **domain of separation** for $\mathcal{I}$.

Any domain of separation is a G-invariant set, as it is a union of orbits. A sequence of increasing (with respect to inclusion) domains of separation gives rise to an ascending chain of polynomial ideals defining their complement. Since any polynomial ring over $\mathbb{C}$ is Noetherian, there exists a maximal domain of separation.

The following proposition details several important properties and non-trivial results about the structure of $\mathbb{C}(\mathcal{Y})^G$ that can be found in [54].

Proposition 2.3.8.

1. The field $\mathbb{C}(\mathcal{Y})^G$ is finitely generated over $\mathbb{C}$.

2. A subset $\mathcal{I} \subset \mathbb{C}(\mathcal{Y})^G$ is generating if and only if it is separating.

3. The transcendental degree of $\mathbb{C}(\mathcal{Y})^G$ equals to $\dim \mathcal{Y} - \max\limits_{p \in \mathcal{Y}} \dim Gp$.

4. If the field $\mathbb{C}(\mathcal{Y})$ is rational[2] and the transcendental degree of $\mathbb{C}(\mathcal{Y})^G$ over $\mathbb{C}$ equals to 1 or 2, then $\mathbb{C}(\mathcal{Y})^G$ is rational over $\mathbb{C}$.

2.3.1 Algebraic curves

Since we are concerned with algebraic curves $\mathbf{X} = V(\mathbf{F}) \subset \mathbb{CP}^2$, in this section and in subsequent chapters we consider only regular actions of algebraic groups G on $\mathbb{CP}^2$. In this case, each element of $g \in G$ is an automorphism of $\mathbb{CP}^2$ and the action induces a homomorphism from G into the automorphism group of $\mathbb{CP}^2$ given by $Aut(\mathbb{CP}^2) = \mathcal{PGL}(3, \mathbb{C})$ [29]. For this reason, we

[2] i.e. isomorphic to a field of rational functions of a finite number of independent variables.

can view any algebraic group G acting regularly on $\mathbb{CP}^2$ as a closed subgroup of the projective general linear group $\mathcal{PGL}(3,\mathbb{C})$.

Definition 2.3.9. The **projective general linear group**, denoted $\mathcal{PGL}(3,\mathbb{K})$, is the quotient group $\mathcal{GL}(3,\mathbb{K})\backslash\{\lambda I\}$ where $\lambda \in \mathbb{K}$ is non-zero and I is the identity matrix. When $\mathbb{K} = \mathbb{C}$ we will also denote the projective general linear group by $\mathcal{PGL}(3)$.

In what follows we assume that G is a closed subgroup of $\mathcal{PGL}(3)$. An element $g \in G$ can be represented by a 3×3 non-singular complex matrix A_g, which is defined up to scaling. For $\mathbf{p} = [x_0 : x_1 : x_2] \in \mathbb{CP}^2$, the action of G on $\mathbb{CP}^2$ is defined by:

$$g \cdot \mathbf{p} = [\phi_0(g,\mathbf{p}) : \phi_1(g,\mathbf{p}) : \phi_2(g,\mathbf{p})], \text{ where } \begin{bmatrix} \phi_0(g,\mathbf{p}) \\ \phi_1(g,\mathbf{p}) \\ \phi_2(g,\mathbf{p}) \end{bmatrix} = A_g \begin{bmatrix} x_0 \\ x_1 \\ x_2 \end{bmatrix}. \tag{2.9}$$

On $\mathbb{C}^2$, we use coordinates (x, y). For an affine point $p = (x, y) \in \mathbb{C}^2$, we use an abbreviation $[1 : p] = [1 : x : y]$ to denote the corresponding projective point. The action (2.9) induces a rational action $\Phi : G \times \mathbb{C}^2 \dashrightarrow \mathbb{C}^2$ given by

$$g \cdot p = \left(\frac{\phi_1(g,[1:p])}{\phi_0(g,[1:p])}, \frac{\phi_2(g,[1:p])}{\phi_0(g,[1:p])} \right). \tag{2.10}$$

Example 2.3.10. An important subgroup of $\mathcal{PGL}(3)$ is the **special Euclidean group**, denoted $\mathcal{SE}(2)$, and is given by

$$\mathcal{SE}(2) = \left\{ \begin{bmatrix} 1 & 0 & 0 \\ a & c & s \\ b & -s & c \end{bmatrix} \middle| \; a,b,c,s \in \mathbb{C},\ c^2 + s^1 = 1 \right\}.$$

When restricted to matrices with real entries, this is isomorphic to the group of translations and rotations of $\mathbb{R}^2$, $\mathcal{SE}(2,\mathbb{R})$, given in Example 2.1.13. Via (2.10) one can check that the action of $\mathcal{SE}(2)$ on $\mathbb{C}^2$ is given by

$$(x, y) \mapsto (cx + sy + a, -sx + cy + b).$$

In addition to $\mathcal{SE}(2)$, we also consider other important subgroups of $\mathcal{PGL}(3)$ in this thesis.

Definition 2.3.11. Two subgroups of $\mathcal{PGL}(3)$ are the **Euclidean group**, denoted $\mathcal{E}(2)$, and the **similarity group**, denoted $\mathcal{S}(2)$. The Euclidean group is given by

$$\mathcal{E}(2) = \left\{ \begin{bmatrix} 1 & 0 & 0 \\ a & c & s \\ b & -s & c \end{bmatrix} \text{ or } \begin{bmatrix} 1 & 0 & 0 \\ a & c & s \\ b & s & -c \end{bmatrix} \;\middle|\; a, b, c, s \in \mathbb{C}\, c^2 + s^2 = 1 \right\}.$$

The similarity group is given by

$$\mathcal{S}(2) = \left\{ \begin{bmatrix} 1 & 0 & 0 \\ a & c & s \\ b & -s & c \end{bmatrix} \;\middle|\; a, b, c, s \in \mathbb{C} \right\}.$$

Both contain $\mathcal{SE}(2)$ as a subgroup. When restricted to matrices with real entries, $\mathcal{E}(2)$ corresponds to the group of rotations and translations $\mathcal{SE}(2, \mathbb{R})$ along with reflections, while $\mathcal{S}(2)$ adds scaling transformations to $\mathcal{SE}(2)$.

Definition 2.3.12. The **affine group**, denoted $\mathcal{A}(2)$, is the subgroup of $\mathcal{PGL}(3)$ that fixes the line of points $[x_0 : x_1 : x_2]$ with $x_0 = 0$, i.e. the group of matrices

$$\mathcal{A}(2) = \left\{ \begin{bmatrix} 1 & 0 & 0 \\ a_3 & a_1 & a_2 \\ a_6 & a_3 & a_5 \end{bmatrix} \;\middle|\; a_i \in \mathbb{C}, a_1 a_5 - a_2 a_4 \neq 0 \right\}.$$

The **special affine group**, $\mathcal{SA}(2)$ is the subgroup of $\mathcal{A}(2)$ such that $a_1 a_5 - a_2 a_4 = 1$. When restricted to real matrices, this gives the group of area-preserving transformations of $\mathbb{R}^2$ (see Example 2.1.14).

The action of G on $\mathbb{CP}^2$ will send irreducible, projective curves to irreducible, projective curves. However the action on $\mathbb{C}^2$ may not be everywhere defined on a curve $X \subset \mathbb{C}^2$. Thus we consider the closure of an affine curve's image under a transformation $g \in G$, denoted $\overline{g \cdot X}$.

Definition 2.3.13. We say that an algebraic curve $X \subset \mathbb{C}^2$ is **G-equivalent** to an algebraic curve $Y \subset \mathbb{C}^2$ if there exists $g \in G$ such that $X = \overline{g \cdot Y}$.

Remark 2.3.14. When X is an irreducible curve with $\deg(X) > 1$, the action of an element $g \in G$ is defined on an open subset of X, and hence the image $g \cdot X$ is an open subset of $\overline{g \cdot X}$. Then clearly $\mathbf{X}$ is G-equivalent to $\mathbf{Y}$ if and only if X is G-equivalent to Y.

Similarly as in Definition 2.1.18 we define the symmetry group of an algebraic curve under G.

Definition 2.3.15. The **symmetry group** of X with respect to G is given by the set of self-equivalences (or *symmetries*) of X in G:

$$\mathrm{Sym}(X, G) = \{g \in G \mid X = \overline{g \cdot X}\}.$$

Note that $\mathrm{Sym}(X, G)$ is a closed algebraic subgroup of G.

Definition 2.3.16. The set of symmetries of X that fix every point of the curve forms the **stabilizer group** of X with respect to G:

$$\mathrm{Stab}(X, G) = \bigcap_{p \in X} G_p.$$

One can show that this is a normal subgroup of $\mathrm{Sym}(X, G)$.

As evidenced Remark 2.3.14, it is advantageous to restrict our attention to irreducible curves of degree greater than one. In this case, the stabilizer group is the trivial subgroup of the symmetry group.

Proposition 2.3.17. For an irreducible curve $X \subset \mathbb{C}^2$ of degree greater than one, the stabilizer group $\mathrm{Stab}(X, G)$ consists of only the identity.

Proof. For $g \in G$ and let $A_g \in \mathcal{GL}(3)$ be any of its representatives. Then a point $p \in \mathbb{C}^2$ is fixed by g if and only if $(1, p)$ is an eigenvector of A_g. Therefore, the set $\mathbb{C}^2_g$ of points fixed by g is the intersection of the affine plane $\{x_0 = 1\}$ with the union of the eigenspaces of the matrix A_g.

There are three possibilities: (1) A_g has three linearly independent eigenvectors, then $\mathbb{C}^2_g$ consists of at most[3] three distinct points, (2) A_g has an eigenspace of dimension 2 and an eigenspace of dimension 1, then $\mathbb{C}^2_g$ consists of at most a line and a point, (3) A_g has an eigenspace of dimension 3, then $\mathbb{C}^2_g = \mathbb{C}^2$.

If $g \in \mathrm{Stab}(X, G)$, then $X \subset \mathbb{C}^2_g$. Since X is irreducible of degree > 1, it follows that $\mathbb{C}^2_g = \mathbb{C}^2$. This implies that A_g is a scalar multiple of the identity matrix and g is the identity element of $\mathcal{PGL}(3)$. □

For this particular class of curves, we further show that the orbits of $\mathrm{Sym}(X, G)$ in X are well-behaved.

Proposition 2.3.18. If X is irreducible of degree greater than one, then $|\mathrm{Sym}(X, G)|$ is infinite if and only if there exists a point $p \in X$ whose orbit under $\mathrm{Sym}(X, G)$ is dense in X.

Proof. Let $H = \mathrm{Sym}(X, G)$. This is an algebraic group acting on X.

($\Rightarrow$) Assume $|H|$ is infinite. Then since H is algebraic, $\dim H > 0$. Let H^0 denote the connected component of H containing the origin. By [52, Ch.1 Prop. 2.2.2], this is a closed normal subgroup of H of finite index and so $\dim H^0 > 0$. By Proposition 2.3.5, for any $p \in X$ the orbit $H^0 p$ is an irreducible quasi-affine subvariety of X.

[3] "At most" because an eigenspace may be parallel to the $\{x_0 = 1\}$ plane.

Since $\dim X = 1$, the dimension of H^0p is either zero or one. If for all $p \in X$, $\dim H^0p = 0$, then $H^0p = \{p\}$ for all $p \in X$ since H^0p is irreducible. In this case, $\mathrm{Stab}(X, G)$ contains H^0, contradicting the statement of Proposition 2.3.17. Therefore, there exists $p \in X$ such that $\dim H^0p = 1$. Since X is irreducible of dimension 1, this implies $\overline{H^0p} = X$.

($\Leftarrow$) Assume there exists a point $p \in X$ whose orbit under H is dense in X. Then $\dim Hp = 1$. By Proposition 2.3.5, $\dim Hp \leq \dim H$. Therefore $\dim H > 0$ and so $|H|$ is infinite. □

Proposition 2.3.19. If X is irreducible of degree greater than one and $|\mathrm{Sym}(X, G)| = n < \infty$, then for all but finitely many points $p \in X$ the orbit under $\mathrm{Sym}(X, G)$ consists of exactly n distinct points.

Proof. Let $H = \mathrm{Sym}(X, G)$. For $g \in H$, define $X_g = \{p \in X \mid g \cdot p = p\}$. From the proof of Proposition 2.3.17 it follows that if $g \neq e$, then X_g is either empty or finite. Consider the set $E_g = \{p \in X \mid g \cdot p \text{ is undefined}\}$, which is also empty or finite. Since $|H|$ is finite, the set $\Delta = \cup_{g \in H}(E_g \cup X_g)$ is empty or finite. For all $p \in X \backslash \Delta$, $g \cdot p$ is defined for all $g \in H$ and the stabilizer $H_p = \{e\}$. Then $|Hp| = |H|/|H_p| = n$. □

In fact the symmetry group of a generic algebraic curve of degree greater than four is trivial. The following proposition follows from [51, Corollary 2.10, Ch. 2] and [51, Theorem 2.8, Ch. 2].

Proposition 2.3.20. For a generic algebraic curve X such that $\deg(X) \geq 4$ the subgroup $\mathrm{Sym}(X, G)$ of G consists of only the identity. For a generic curve X of degree 3, $\mathrm{Sym}(X, G)$ is finite.

CHAPTER 3

Differential signatures of algebraic curves

We start the chapter by introducing the notion of a classifying pair of rational differential invariants and establish their existence for the action of the projective group and its subgroups on $\mathbb{C}^2$ given by (2.10). We show that a classifying pair of rational differential invariants allows one to construct a signature map for non-exceptional, irreducible algebraic curves. The Zariski closure of the image of a curve under the signature map is the curve's *signature curve*, and its implicit equation is the *signature polynomial*. A curve's signature curve, and hence its signature polynomial, characterizes the curve's equivalence class, i.e. two curves are G-equivalent if and only if they have the same signature curve. We show that the signature map is related to the size of a curve's symmetry group: the signature map is generically $n : 1$ when the symmetry group is finite and constant when it is infinite.

In Section 3.2 we derive a formula for the degree of the signature polynomial and also provide bounds for this degree. We also provide a formula and bounds for the degree of the signature polynomial in each variable. Given a set of classifying invariants, for a generic curve of fixed degree we show that the signature polynomials share the same monomial support and genus. In particular there exists a 'generic degree' and 'generic genus' of the signature polynomials of curves of fixed degree. The chapter concludes with a discussion of how the results shown here connect to the group equivalence problem for *real* algebraic curves and some examples of using the degree formula and bounds to study signatures of algebraic curve.

In this chapter we make the following assumptions when referring to groups G or curves X:

1. A group G is a closed subgroup of $\mathcal{PGL}(3)$ with $\dim G > 0$.

2. The rational action of G on $\mathbb{C}^2$ is defined by (2.9) and (2.10).

3. $X \subset \mathbb{C}^2$ is an irreducible algebraic curve of degree greater than one.

3.1 Signatures of algebraic curves

3.1.1 Differential invariants and algebraic curves

To define differential invariants and the action of a group on the derivatives of a curve, we introduce the notion of the *jet space* of planar curves. Since we assume that a curve $X \subset \mathbb{C}^2$ is of degree greater than one, any curve will have finitely many vertical tangencies, and the derivatives of y with respect to x are well-defined on an open subset of X, i.e. for all but finitely many points of X.

Explicitly, for $X = V(F)$ and any point $p = (p_1, p_2) \in X$ where $F_y(p) \neq 0$, the curve X agrees in some neighborhood of p with the graph of an analytic function $y = f(x)$. Then for a positive integer n, we can define $y_X^{(n)}(p) = f^{(n)}(p_1)$ to be the n-th derivative of $f(x)$ at $x = p_1$.

Remark 3.1.1. For each $n \in \mathbb{Z}_+$, $y_X^{(n)}$ is a rational function on X that, using the implicit differentiation, can be written as a rational function of partial derivatives of F. For example,

$$\begin{aligned} & F(x,y) = 0 \\ (\Rightarrow)\ & \frac{d}{dx}(F(x,y)) = 0 \\ (\Rightarrow)\ & F_x(x,y) + F_y(x,y)y^{(1)} = 0 \\ (\Rightarrow)\ & y_X^{(1)} = \frac{-F_x}{F_y}. \end{aligned}$$

By again differentiating both sides assuming y as a function of x, and using the fact that $y_X^{(1)} = \frac{-F_x}{F_y}$ we find that

$$y_X^{(2)} = \frac{-F_{xx}F_y^2 + 2F_{xy}F_xF_y - F_{yy}F_x^2}{F_y^3}.$$

One can continue this process to find $y_X^{(n)}$ as a rational function of the partial derivatives of F for any $n \in \mathbb{Z}_+$. In fact one can check that each derivative function can be written as

$$y^{(n)}|_X = \frac{P_n(x,y)}{(F_y)^{2n-1}} \quad \text{where } P_n \in \mathbb{Q}\left[\frac{\partial^{i+j}F}{\partial x^i \partial y^j} \ : \ i+j \leq n\right]$$

and $P_n(x,y)$ is a polynomial of degree $(2n-1)d-(3n-2)$.

The coordinate functions on the *n-th jet space* of planar curves J^n are denoted by $(x, y, y^{(1)}, \ldots, y^{(n)})$. Although formally $y^{(k)}$ is viewed as an independent coordinate function, we can think of J^n as $\mathbb{C}^{n+2}$, since $y_X^{(n)}$ is defined on an open subset of X and we can safely ignore the points where X has a vertical tangency.

Definition 3.1.2. The *n-th jet* of a curve $X \subset \mathbb{C}^2$, denoted $X^{(n)}$, is the algebraic closure of the image of X under the rational map $j_X^n : X \dashrightarrow J^n$, where for $p \in X$,

$$j_X^n(p) = (x(p), y(p), y_X^{(1)}(p), \ldots, y_X^{(n)}(p)).$$

In this way we can consider a curve $X \subset \mathbb{C}^2$ as a curve in the higher dimensional space J^n. The action of G on planar curves induces a *prolonged* action of G on J^n.

Definition 3.1.3. Let G act on $\mathbb{C}^2$. For $g \in G$, let $(\overline{x}, \overline{y}) = g \cdot (x, y)$. *The prolongation of the G-action from* $\mathbb{C}^2$ *to* J^n is a rational action defined by

$$g \cdot (x, y, y^{(1)}, \ldots, y^{(n)}) = (\overline{x}, \overline{y}, \overline{y}^{(1)}, \ldots, \overline{y}^{(n)})$$

where

$$\overline{y}^{(1)} = \frac{\frac{d}{dx}\left[\overline{y}(g,x,y)\right]}{\frac{d}{dx}\left[\overline{x}(g,x,y)\right]} \quad \text{and} \quad \overline{y}^{(k+1)} = \frac{\frac{d}{dx}\left[\overline{y}^{(k)}(g,x,y,y^{(1)},\ldots,y^{(k)})\right]}{\frac{d}{dx}\left[\overline{x}(g,x,y)\right]} \text{ for } k = 1, \ldots, n-1.$$

The operator $\frac{d}{dx}$ is the *total derivative operator*. This is the unique $\mathbb{C}$-linear operator mapping $C(J^n) \to C(J^{n+1})$ for $n \geq 0$ satisfying the product rule, $\frac{d}{dx}(x) = 1$, and $\frac{d}{dx}(y^{(k)}) = y^{(k+1)}$ for $k \geq 0$. Here we use the convention that $y = y^{(0)}$ and coordinate functions of g are considered to be constant with respect to x.

This action is defined so that the following fundamental property holds:

$$j_{g\cdot X}^n(g \cdot p) \;=\; g \cdot j_X^n(p) \;\text{ for all } g \in G \text{ and } p \in X \text{ where } g \cdot p \text{ is defined.} \tag{3.1}$$

In particular, the n-th jet of the image of X under the action of $g \in G$ coincides with the image of the n-th jet of X under the prolonged action of g:

$$\overline{g \cdot X^{(n)}} = \overline{(g \cdot X)^{(n)}}. \tag{3.2}$$

The n-th jet of a curve X gives us a way to restrict differential functions, particularly differential invariants to X.

Definition 3.1.4. A rational function $K(x, y, y^{(1)}, \ldots, y^{(n)})$ on J^n is called a **rational differential function**. The **differential order** of K is the maximal k, such that K explicitly depends on $y^{(k)}$:

$$\operatorname{ord}(K) = \max_i \left\{ i \,\middle|\, \frac{\partial K}{\partial y^{(i)}} \neq 0 \right\}.$$

If K is invariant under the prolonged action it is called a **rational differential invariant**.

Note that if $\operatorname{ord}(K) = k$, then $K \in \mathbb{C}(J^n)$ for all $n \geq k$.

Definition 3.1.5. For a curve X, the *restriction* of a differential function K to X is denoted $K|_X$ and defined by the composition, $K|_X = K \circ j^n_X$.

If K is a *rational* differential function on J^n, then $K|_X$ is a rational function on X, and we can obtain the explicit formula for $K|_X$ as a rational function of x and y by substituting the expressions $y^{(1)}_X, \ldots, y^{(n)}_X$ obtained as in Remark 3.1.1 for coordinates $y^{(1)}, \ldots, y^{(n)}$. This also shows that $K|_X$ is a rational function of the partial derivatives of F for $X = V(F)$.

3.1.2 Classifying differential invariants

For smooth curves Theorem 2.1.26 guarantees the existence of G-invariant curvature, a differential invariant which is a smooth function on the jet space of the curve. G-invariant curvature and its derivative with respect to G-invariant arc length then define a signature map as in Definiton 2.1.27.

Our goal in this section will be to show the existence of two *rational* differential invariants that define a signature map for algebraic curves in $\mathbb{CP}^2$ under the regular action of an algebraic group G. We use the same definition as was given in [10, Section 4, Definition 7] in the real case for a *classifying* pair of differential invariants that we will use to construct the signature map.

Definition 3.1.6. Let r-dimensional algebraic group G act on $\mathbb{C}^2$ and K_1, K_2 be *rational differential invariants* of orders $k \leq r-1$ and r, respectively. The set $\mathcal{I} = \{K_1, K_2\}$ is called **classifying** if K_1 is separating on J^k and $\mathcal{I}$ is separating on J^r.

We start by showing, in Theorem 3.1.9, that the field $\mathbb{C}(J^r)^G$ of rational invariants of the order at most $r = \dim G$ has a very simple structure. The following is a formulation in our context of an important result originally due to Ovsiannikov [49] (see also [45, Theorem 5.11]).[1]

[1] This result is true under the assumption that G is a closed subgroup of $\mathcal{PGL}(3)$ with action on $\mathbb{C}^2$ defined in (2.10), implying that this action is effective. For general actions of algebraic groups on algebraic varieties one needs to assume local effectiveness of the action (the set of elements in G with a trivial action is finite). The theorem was originally stated for Lie groups acting on smooth (non-algebraic) real manifolds, and in this setting, as was shown in [47], a stronger assumption of local effectiveness on all open subsets is required. The proof remains valid over $\mathbb{C}$.

Proposition 3.1.7. Let a group G of dimension r act on $\mathbb{C}^2$. Then there exists a $k \geq 0$ such that, for all $n \geq k$, the maximal orbit dimension of the prolonged action on J^n is r.

The following lemma shows that we can build higher order differential invariants from lower order invariants.

Lemma 3.1.8. Assume K_1 and K_2 are two algebraically independent rational differential invariants, such that $\max\{\operatorname{ord}(K_1), \operatorname{ord}(K_2)\} = k$. Then

$$\frac{dK_2}{dK_1} := \frac{\frac{dK_2}{dx}}{\frac{dK_1}{dx}}$$

is a rational differential invariant of order $k+1$.

Proof. From [45, Prop. 5.15], the lemma is true for functionally independent differential invariants. The result then follows from the Jacobian criterion of independence, which states that polynomials over an algebraically closed field are algebraically independent if and if only their Jacobian is generically of full rank (this implies that K_1 and K_2 are functionally independent).

Consider the collection of polynomials $\mathcal{F} = \{f_1, \ldots, f_s\} \subset \mathbb{C}[x_1, \ldots, x_n]$. If $\mathcal{F}$ is algebraically dependent then there exists some $F \in \mathbb{C}[x_1, \ldots, x_s]$ such that $F(f_1, \ldots, f_s) = 0$. Let $J_{\mathcal{F}}$ denote the Jacobian of $\mathcal{F}$; then by the chain rule $J_{\mathcal{F}}(p) \cdot \nabla F(p)$ for any $p \in \mathbb{C}^n$. If $\mathcal{F}$ is an algebraically independent set, then the image of the regular map $f = (f_1, \ldots f_s)$ is dense in $\mathbb{C}^s$. This implies that the differential map $d_x f$ is surjective on an open subset of $\mathbb{C}^n$, further implying the Jacobian is generically of full rank [50, Ch. 2, Sec. 6]. □

Theorem 3.1.9. Let $\dim G = r$, then the field of $\mathbb{C}(J^r)^G$ of rational invariants on J^r is a rational field of transcendental degree two. In other words, there exists two rational invariants K_1 and K_2 such that

$$\mathbb{C}(J^r)^G = \mathbb{C}(K_1, K_2). \tag{3.3}$$

Moreover K_1 and K_2 can be chosen so that K_1 is of differential order k, strictly less than r, and K_2 is of differential order r. In addition, the field $\mathbb{C}(J^k)^G$ of rational invariants on J^k is a rational field of transcendental degree one and

$$\mathbb{C}(J^k)^G = \mathbb{C}(K_1). \tag{3.4}$$

Proof. The dimension of an orbit can not exceed the dimension of the group. Therefore, since $\dim J^{r-1} = r+1$, the transcendental degree of $\mathbb{C}(J^{r-1})^G$ is at least 1 by Part 3. of Proposition 2.3.8. Thus there exists a rational invariant K_1 such that $\operatorname{ord}(K_1) = k_1 < r$. We may assume that the order k_1 of K_1 is minimal among all such invariants. Similarly, since $\dim J^r = r+2$, the transcendental degree of $\mathbb{C}(J^{r-1})^G$ is at least 2, and there exists a rational

invariant K_2, algebraically independent from K_1, such that $\operatorname{ord}(K_2) = k_2 \leq r$. By the minimality assumption on k_1, we have $k_1 \leq k_2$. Assume that $k_2 < r$. By Proposition 3.1.8, invariant $H_1 = \frac{dK_2}{dK_1}$ is of order $k_2 + 1$. For $i > 1$, we define invariants $H_i = \frac{dH_{i-1}}{dK_1}$.

The $n+2$ invariants $K_1, K_2, H_1, H_2, \ldots, H_n$ are of orders $k_1, k_2, k_2+1, \ldots k_2+n$, respectively. Since K_1 and K_2 are independent, and each subsequent invariant contains a new jet variable, the gradients of these invariants as functions on J^{k_2+n} are independent, and hence the invariants are independent. Therefore the maximal orbit dimension on J^{k_2+n} does not exceed $\dim J^{k_2+n} - (n+2) = k_2$. Since n can be arbitrary large, it follows from Proposition 3.1.7 that $k_2 = r$. In summary, we proved so far

$$k_1 < k_2 = r$$

and that there are no differential invariants of orders strictly less than k_1, or strictly between k_1 and r.

Assume that there is an invariant K_3 of order r, independent of K_1 and K_2. Then by similar argument as in the above paragraph, the $n+3$ invariants $K_1, K_2, K_3, H_1, H_2, \ldots, H_n$ of orders $k_1, r, r, r+1, \ldots r+n$, respectively, are independent for all n. It follows that the maximal orbit dimension on J^{r+n} does not exceed $\dim J^{r+n} - (n+3) = r-1$ for all n. This contradicts Proposition 3.1.7.

We conclude that the transcendental degree of $\mathbb{C}(J^k)^G$ is 1 and the transcendental degree of $\mathbb{C}(J^r)^G$ is 2. Then (3.3) and (3.4) follow from Part 4 of Proposition 2.3.8. □

Remark 3.1.10. In fact, from Theorem 5.24 in [45] and Sophus Lie's classification of all infinitesimal group actions on the plane (see Table 5 in [45]) it follows that there are only three possibilities for the differential order k of the lower order classifying invariant K_1, namely $k = r-1$, $k = r-2$ and $k = 0$.

For most of the actions (and all actions considered in Chapter 4) $k = r-1$. The case $k = 0$ occurs if and only if the action G is intransitive on $\mathbb{C}^2$. An example of such action is the action of a 2-dimensional subgroup of $\mathcal{PGL}(3)$, given by $(x, y) \to (\lambda x + a, y)$, where $\lambda \in \mathbb{C}^*$ is non-zero and $a \in \mathbb{C}$.

Among subgroups of $\mathcal{PGL}(3)$, the third possibility, $k = r-2 \neq 0$, occurs only for two actions: (1) a three-dimensional subgroup acting by $(x, y) \to (\lambda x + a, \lambda y + b)$, where $\lambda \in \mathbb{C}^*$ and $a, b \in \mathbb{C}$ and (2) a four-dimensional subgroup acting by $(x, y) \to (\lambda x + a, cx + \lambda^2 y + b)$, where $\lambda \in \mathbb{C}^*$ and $a, b, c \in \mathbb{C}$

Theorem 3.1.11. For any action of G on $\mathbb{C}^2$ there exists a classifying set $\mathcal{I} = \{K_1, K_2\}$ of differential invariants. Moreover the set $\mathcal{I}$ is classifying if and only if $\mathcal{I}$ generates the field $\mathbb{C}(J^r)^G$ of rational differential invariants of order $r = \dim G$ and K_1 generates the field $\mathbb{C}(J^k)^G$ of rational invariants of order $k < r$.

Proof. This result follows immediately from Theorem 3.1.9 and Part 2 of Proposition 2.3.8. □

Proposition 3.1.12. Let $\mathcal{I} = \{K_1, K_2\}$ be a classifying set of differential invariants for the action of G on $\mathbb{C}^2$. Then $\tilde{K_1}$ is of the form

$$\tilde{K_1} = \frac{aK_1 + b}{cK_1 + d} \tag{3.5}$$

and $\tilde{K_2}$ is of the form

$$\tilde{K_2} = \frac{\alpha(K_1)K_2 + \beta(K_1)}{\gamma(K_1)K_2 + \delta(K_1)}, \tag{3.6}$$

for some $a, b, c, d \in \mathbb{C}$ and $\alpha, \beta, \gamma, \delta \in \mathbb{C}(K_1)$ such that $ad - bc, \alpha(K_1)\delta(K_1) - \beta(K_1)\gamma(K_1) \neq 0$ if and only if $\tilde{\mathcal{I}} = \{\tilde{K_1}, \tilde{K_2}\}$ is a classifying set of differential invariants for the action of G on $\mathbb{C}^2$.

Proof. Note that by Part 4 of Proposition 2.3.8 and Theorem 3.1.11, then $\mathcal{I} = \{K_1, K_2\}$ is a classifying pair of differential invariants if and only if $\mathbb{C}(K_1) = \mathbb{C}(J^k)^G$ and $\mathbb{C}(K_1, K_2) = \mathbb{C}(J^r)^G$ for some $k < r$ where $r = \dim(G)$.

We start with the reverse direction. If $\tilde{\mathcal{I}}$ is also a classifying pair of differential invariants, then $\mathbb{C}(\tilde{K_1}) = \mathbb{C}(J^k)^G = \mathbb{C}(K_1)$. Since $\mathbb{C}(K_1) \cong \mathbb{C}(\tilde{K_1})$, there exists an automorphism ϕ of $\mathbb{C}(K_1)$, fixing $\mathbb{C}$, such that $\phi(K_1) = \tilde{K_1}$. In this case ϕ is given by (3.5) (see [36, Example, Sec. 5.2] or [18, Exer. 14.1.8]). A similar argument along with the fact that $\mathbb{C}(K_1)(K_2) = \mathbb{C}(K_1, K_2)$ shows that $\tilde{K_2}$ must be of the form given in (3.6).

The forward direction follows from the fact that (3.5) and (3.6) define automorphisms of $\mathbb{C}(K_1)$ and $\mathbb{C}(K_1, K_2)$ respectively. □

3.1.3 Signature Map

We will now show that from a classifying pair of invariants, whose existence is guaranteed in Theorem 3.1.11, we can build a signature map for what we call *non-exceptional* algebraic curves. In this section we assume that $\dim(G) = r$ and that $\mathcal{I} = \{K_1, K_2\}$ are a classifying set of differential invariants with $ord(K_1) = k < r = ord(K_2)$.

Definition 3.1.13. Let $\mathcal{I} = \{K_1, K_2\}$ be a classifying set of rational differential invariants for a group G of dimension r. Let $\mathrm{ord}(K_1) = k$ and let $W_1 \subset J^k$ be a maximal domain of separation for $\{K_1\}$ and $W_2 \subset J^r$ be a maximal domain of separation for $\mathcal{I}$. Then, for $X \subset \mathbb{C}^2$, a point $p \in X$ is called *$\mathcal{I}$-regular* if

(a) $j^r_X(p)$ is defined;

(b) $j^k_X(p) \in W_1$ and $j^r_X(p) \in W_2$;

(c) $\frac{\partial K_1}{\partial y^k}|_{j_X^k(p)} \neq 0$ if K_1 is constant on X, and $\frac{\partial K_2}{\partial y^{(r)}}|_{j_X^r(p)} \neq 0$ otherwise.

The condition that $j_X^r(p)$ is defined can equivalently be stated as $F_y(p) \neq 0$ where $F(x,y)$ is the polynomial whose zero set equals X. Thus singular points of X are not $\mathcal{I}$-regular.

Definition 3.1.14. A complex algebraic curve $X \subset \mathbb{C}^2$ is called **non-exceptional** with respect to a classifying set of differential invariants, $\mathcal{I}$, if all but a finite number of its points are $\mathcal{I}$-regular.

True to their name, the set of non-exceptional curves of fixed degree d is dense in the set of all curves of degree d.

Lemma 3.1.15. Let d, n be positive integers satisfying $n \leq \binom{d+2}{2} - 2$. For a generic point $a = (a_0, \ldots, a_n) \in \mathbb{C}^{n+1}$, there exists an algebraic curve $X \subset \mathbb{C}^2$ of degree d for which $(0, a_0) \in X$ and $j_X^{(n)}(0, a_0) = (0, a_0, \ldots, a_n)$.

Proof. Consider the subset $\mathcal{Y}$ of $\mathbb{P}(\mathbb{C}[x,y]_{\leq d}) \times \mathbb{C}^{n+1}$ consisting of pairs $([F], a)$ for which F is irreducible of degree d, $F(0, a_0) = 0$, $F_y(0, a_0) \neq 0$, and $j_{V(F)}^{(n)}(0, a_0) = (0, a_0, \ldots, a_n)$. Since $j_{V(F)}^{(n)}$ is a rational function of both the points of $V(F)$ and the coefficients of F, as seen in Remark 3.1.1, this is a quasi-projective variety. The conditions $F(0, a_0) = 0$ and $a_k = y_X^{(k)}(0, a_0)$ are algebraically independent, since each involves a new variable, a_k.

From this, it follows that $\mathcal{Y}$ has codimension $n+1$ in $\mathbb{P}(\mathbb{C}[x,y]_{\leq d}) \times \mathbb{C}^{n+1}$ and thus dimension $\binom{d+2}{2} - 1$. The projection of $\mathcal{Y}$ onto $\mathbb{C}^{n+1}$ is therefore an open subset of an affine variety. It either contains a nonempty Zariski-open set or is contained in a hypersurface in $\mathbb{C}^{n+1}$. We need to rule out the latter when $n \leq \binom{d+2}{2} - 2$.

Suppose for the sake of contradiction that for some $n \leq \binom{d+2}{2} - 2$, there is a polynomial relation $P(y, y^{(1)}, \ldots, y^{(n)}) = 0$ that holds for every point on the image of $X \cap V(x)$ under $j_X^{(n)}$ for every irreducible curve X of degree d. Without loss of generality, we can assume that n is the minimal integer for which this holds and that the polynomial P is irreducible.

Then, by Bertini's theorem, for generic $a_0, \ldots, a_{n-1} \in \mathbb{C}$, $P(a_0, \ldots, a_{n-1}, y^{(n)})$ is a non-zero polynomial in $y^{(n)}$ with simple roots, around which $y^{(n)}$ is an analytic function of $a_0, \ldots, a_{n-1}$. Due to the uniqueness theorem for the solutions of complex ODEs [37], for any such $a_0, \ldots, a_{n-1}$ and a_n with $P(a_0, \ldots, a_n) = 0$, there exists a unique solution $y = f(x)$ to the differential equation $P(y, y^{(1)}, \ldots, y^{(n)}) = 0$ satisfying the initial conditions $x = 0$, $f(0) = a_0$, and $f^{(k)}(0) = a_k$ for $k = 1, \ldots, n$.

If there exists an irreducible polynomial $F \in \mathbb{C}[x,y]$ of degree d for which $F(x, f(x))$ is identically zero, then F is unique up to scaling. This means that every point in the projection of $\mathcal{Y}$ onto $\mathbb{C}^{n+1}$ has at most one preimage. Since the projection has dimension $\leq n$, this implies that the dimension of $\mathcal{Y}$ is also at most n, which contradicts the calculation that $\dim(\mathcal{Y})$ equals $\binom{d+2}{2} - 1 > n$. Therefore the projection of $\mathcal{Y}$ onto $\mathbb{C}^{n+1}$ must be Zariski-dense. $\square$

Theorem 3.1.16. Let $\mathcal{I}$ be a G-classifying set of rational differential invariants for the action of a group G. Then for $d \in \mathbb{Z}_+$ with $\binom{d+2}{2} - 2 \geq \dim(G)$, a generic plane curve of degree d is non-exceptional with respect to $\mathcal{I}$.

Proof. For an irreducible curve X, the $\mathcal{I}$-regular points form a Zariski-open subset of X, as seen in Definition 3.1.13. Either this is all but finitely-many points of X, in which case X is non-exceptional, or empty, meaning that no points of X are $\mathcal{I}$-regular. In particular, if all intersection points of X with $V(x)$ are $\mathcal{I}$-regular, then X is non-exceptional.

Indeed, the condition that a point p is $\mathcal{I}$-regular on X is equivalent to the jet $j_X^{(r)}(p)$ belonging to a Zariski-open subset $\mathcal{U}$ of $J^r \cong \mathbb{C}^{r+2}$, where $r = \dim(G)$. Consider the quasi-projective variety $\mathcal{Y}$ defined in the proof of Lemma 3.1.15 with $n = r$. Its intersection with $\mathbb{P}(\mathbb{C}[x,y]_{\leq d}) \times \mathcal{U}$ is an open subset of $\mathcal{Y}$, which is nonempty by Lemma 3.1.15.

Furthermore, the projection of $\mathcal{Y}$ onto $\mathbb{P}(\mathbb{C}[x,y]_{\leq d})$ is dominant (i.e. the image in Zariski-dense). Specifically, consider the open dense set of irreducible polynomials $F \in \mathbb{C}[x,y]_{\leq d}$ for which $F(0,y)$ has a simple root $y = a_0$ at which $F_y(0,a_0)$ is nonzero. For any such F, $([F], a)$ belongs to $\mathcal{Y}$, where $j_{V(F)}^{(r)}(0,a_0) = (0,a)$. It follows that the projection of the set $\mathcal{Y} \cap (\mathbb{P}(\mathbb{C}[x,y]_{\leq d}) \times \mathcal{U})$ onto $\mathbb{P}(\mathbb{C}[x,y]_{\leq d})$ is also dominant. Therefore, for a generic plane curve of degree d, the points $X \cap V(x)$ are $\mathcal{I}$-regular in X, and thus X is non-exceptional. □

Furthermore the set of non-exceptional curves for a given set of classifying invariants $\mathcal{I}$ is a G-invariant set.

Lemma 3.1.17. If X is non-exceptional then so is $Y = \overline{g \cdot X}$ for all $g \in G$.

Proof. We check that if conditions (a) – (c) in Definition 3.1.13 are satisfied by all but finitely many points on X, then the same is true for Y.

(a) Assume that there are at most finitely many points $p \in X$, such that $j_X^r(p)$ is undefined (equivalently $F_y(p) = 0$, where F is a defining polynomial of X). This is, in fact, true for any irreducible curve of degree greater than 1. Since the action of G preserves these properties, there are at most finitely many points $p \in Y$, such that $j_Y^r(p)$ is undefined.

(b) Assume that there are at most finitely many points $p \in X$, such that $j_X^k(p) \notin W_1$ and $j_X^r(p) \notin W_2$. From the G-invariance of W_1 and W_2 and (3.1), combined with the fact that $Y \backslash (g \cdot X)$ is a finite set, it follows that there are at most finitely many points $p \in Y$ such that $j_Y^k(p) \notin W_1$ and $j_Y^r(p) \notin W_2$.

(c) We start by showing that if K is a differential invariant of order n, then the set of points $p^{(n)} \in J^n$ where $\frac{\partial K}{\partial y^{(n)}}(p^{(n)}) \neq 0$ is G-invariant. Since K is invariant, $K(p^{(n)}) = K(g \cdot p^{(n)})$, whenever both sides are defined, and the differentiation with respect $y^{(n)}$using the chain rule

yields:

$$\begin{aligned}
&\frac{\partial K}{\partial y^{(n)}}\left(p^{(n)}\right)\\
&= \frac{\partial K}{\partial \overline{x}}\left(g\cdot p^{(n)}\right)\frac{\partial \overline{x}}{\partial y^{(n)}}\left(p^{(n)}\right) + \frac{\partial K}{\partial \overline{y}}\left(g\cdot p^{(n)}\right)\frac{\partial \overline{y}}{\partial y^{(n)}}\left(p^{(n)}\right) + \ldots + \frac{\partial K}{\partial \overline{y}^{(n)}}\left(g\cdot p^{(n)}\right)\frac{\partial \overline{y}^{(n)}}{\partial y^{(n)}}\left(p^{(n)}\right)\\
&= \frac{\partial K}{\partial \overline{y}^{(n)}}\left(g\cdot p^{(n)}\right)\frac{\partial \overline{y}^{(n)}}{\partial y^{(n)}}\left(p^{(n)}\right).
\end{aligned}$$

The last equality follows from the fact that the functions $\overline{x}, \overline{y}$, and $\overline{y}^{(i)}$, given in Definition 3.1.3, do not depend on $y^{(n)}$ for $i = 1, \ldots, n-1$. Thus if $\frac{\partial K}{\partial y^{(n)}}(p^{(n)}) \neq 0$, so does every point in the orbit of $p^{(n)}$.

Condition (c) states that, if K_1 is constant on X, then for all but finitely many $p \in X$, $\frac{\partial K_1}{\partial y^k}|_{j^k_X(p)} \neq 0$, otherwise for all but finitely many $p \in X$, $\frac{\partial K_2}{\partial y^r}|_{j^r_X(p)} \neq 0$, where $k = \operatorname{ord}(K_1)$ and $r = \operatorname{ord}(K_2)$. Due to (3.1), and G-invariance property showed above, the same is true for Y. □

For a non-exceptional algebraic curve $X \subset \mathbb{C}^2$, we define the signature and signature map in a similar manner as in the case of smooth curves (see Definition 2.1.27).

Definition 3.1.18. Let $\mathcal{I} = \{K_1, K_2\}$ be a classifying set of rational differential invariants with respect to the action G, and let $X \subset \mathbb{C}^2$ be a non-exceptional curve. Then the rational map $\sigma_X : X \dashrightarrow \mathbb{C}^2$ with coordinates $(K_1|_X, K_2|_X)$ is called the **signature map**. The image of $\mathcal{S}_X = \sigma_X(X)$ is called the **signature** of X.

Note that since X is irreducible, then the closure $\overline{\mathcal{S}_X}$ is also an irreducible variety of dimension 0 or 1. If $\dim(\overline{\mathcal{S}_X}) = 0$, then it is a single point and, therefore, σ_X is a constant map. If $\dim(\overline{\mathcal{S}_X}) = 1$, then it is an irreducible planar curve, which we call the *signature curve* of X. An irreducible polynomial vanishing on $\overline{\mathcal{S}_X}$ is called a *signature polynomial* and is denoted by S_X and it is unique up to scaling by a non-zero constant. Since the signature map is constructed using differential invariants, the following proposition may not be surprising.

Proposition 3.1.19. Assume that $X, Y \subset \mathbb{C}^2$ are G-equivalent and non-exceptional with respect to a classifying set of rational differential invariants $\mathcal{I} = \{K_1, K_2\}$. Then $\overline{\mathcal{S}_X} = \overline{\mathcal{S}_Y}$.

Proof. If X and Y are G-equivalent, then there exists $g \in G$ such that $Y = \overline{g \cdot X}$. Due to the fundamental property of prolongation (3.1), we have $j^r_Y(q) = g \cdot j^r_X(p)$, for any $p \in X$ where $q = g \cdot p$ is defined. Since K_1 and K_2 are invariant, we have

$$K_1(j^r_X(p)) = K_1(j^r_Y(q)) \text{ and } K_2(j^r_X(p)) = K_2(j^r_Y(q)).$$

This implies $\sigma_X(p) = \sigma_Y(q)$. Since $g \cdot p$ is defined for all but finitely many points in X and $g \cdot X$ is dense in Y, this implies that $\overline{\mathcal{S}_X} = \overline{\mathcal{S}_Y}$. □

We will gradually work towards proving the converse of the above statement. This will show that the *Zariski closure* of the signatures, and thus the signature polynomials, characterize the equivalence classes of curves. We will also show the relationship between the cardinality of the preimage of a generic point under a signature map and the cardinality of the symmetry group. For both of these results we need several lemmas.

Lemma 3.1.20. Let $\mathcal{I} = \{K_1, K_2\}$ be a classifying set of rational differential invariants with respect to the action G, and let $X, Z \subset \mathbb{C}^2$ be two non-exceptional curves, such that the restrictions of K_1 to both curves equal to the same constant function:

$$K_1|_X = K_1|_Z = c.$$

If there exists $p \in X \cap Z$ such that

1. $j^k_X(p) = j^k_Z(p)$, where $k = \mathrm{ord}(K_1)$,
2. p is not exceptional for X,

then $X = Z$.

Proof. Since p is non-singular for both X and Z, in some neighborhood of p, curves X and Z coincide with the graphs of analytic functions $y = f(x)$ and $y = g(x)$, respectively. Both $y = f(x)$ and $y = g(x)$ are solutions of the differential equation

$$K_1(x, y, y^{(1)}, \ldots, y^{(k)}) = c, \tag{3.7}$$

with the same initial condition described by the point $j^k_X(p) = j^k_Z(p)$. Since p is non-exceptional, $\frac{\partial K_1}{\partial y^k}|_{j^k_X(p)} \neq 0$, and so using the implicit function theorem, (3.7) can be rewritten as $y^{(k)} = H(x, y, y^{(1)}, \ldots, y^{(k-1)})$ in a neighborhood of $j^k_X(p)$, where H is an analytic function of the jet coordinates. We can now invoke the uniqueness theorem for the solutions of complex ODEs [37] to conclude that $f(x) = g(x)$. Therefore X and Z coincide on a positive dimensional subset. Since they are irreducible $X = Z$. □

Lemma 3.1.21. Let $\mathcal{I} = \{K_1, K_2\}$ be a classifying set of rational differential invariants with respect to the action G, and let $X, Z \subset \mathbb{C}^2$ be two non-exceptional curves with the same signature curves, $\overline{\mathcal{S}_X} = \overline{\mathcal{S}_Z}$. If there exists $p \in X \cap Z$ such that

1. $j^r_X(p) = j^r_Z(p)$,
2. p is not exceptional for X
3. if $\dim \mathcal{S}_X > 0$ and $S_X(\kappa_1, \kappa_2)$ is the signature polynomial, then $\frac{\partial S}{\partial \kappa_2}|_{\sigma_X(p)} \neq 0$,

then $X = Z$.

Proof. If σ_X (and, therefore, σ_Z) is a constant map, then there exists $c \in \mathbb{C}$, such that $K_1|_X = c$ and $K_1|_Z = c$. Then we are in the situation of Lemma 3.1.20 and the conclusion follows. Otherwise, σ_X and, σ_Z define the same signature polynomial $S_X(\kappa_1, \kappa_2) = S_Z(\kappa_1, \kappa_2) := S(\kappa_1, \kappa_2)$. Since p is non-singular for both X and Z, in some neighborhood of p, curves X and Z coincide with the graphs of analytic functions $y = f(x)$ and $y = g(x)$, respectively. Both $y = f(x)$ and $y = g(x)$ are solutions of the differential equation

$$S\left(K_1(x, y, y^{(1)}, \dots, y^{(k)}), K_2(x, y, y^{(1)}, \dots, y^{(r)})\right) = 0 \tag{3.8}$$

with the same initial condition described by the point $j^r_X(p) = j^r_Z(p)$. By assumption, $\frac{\partial S}{\partial \kappa_2}|_{\sigma_X(p)}$ and $\frac{\partial K_2}{\partial y^{(r)}}|_{j^r_X(p)}$ are both nonzero. Then using the implicit function theorem, (3.8) can be rewritten as $y^{(r)} = H(x, y, y^{(1)}, \dots, y^{(r-1)})$ in a neighborhood of $j^r_X(p)$, where H is an analytic function of the jet coordinates. As in the previous lemma, we invoke the uniqueness theorem for the solutions of ODEs, to conclude $X = Z$. □

Lemma 3.1.22. Let $\mathcal{I} = \{K_1, K_2\}$ be a classifying set of rational differential invariants with respect to the action G, and let X be a non-exceptional curve. Let $p, q \in X$ be two non-exceptional points, such that

1. $\sigma_X(p) = \sigma_X(q)$
2. if $\dim \mathcal{S}_X > 0$ and $S_X(\kappa_1, \kappa_2)$ is the signature polynomial, then $\frac{\partial S}{\partial \kappa_2}|_{\sigma_X(p)} \neq 0$.

Then there exists $g \in \mathrm{Sym}(X, G)$, such that $q = gp$.

Proof. Since, $\sigma_X(p) = \sigma_X(q)$ we have

$$K_1(j^r_X(p)) = K_1(j^r_X(q)) \text{ and } K_2(j^r_X(p)) = K_2(j^r_X(q)).$$

Since $\mathcal{I}$ is a separating set, and p and q are non-exceptional, there exists $g \in G$, such that $j^r_X(p) = g \cdot j^r_X(q)$. Consider a curve $Z = \overline{g \cdot X}$. By Lemma 3.1.17, Z is non-exceptional. Condition $\overline{\mathcal{S}_X} = \overline{\mathcal{S}_Z}$ holds due to Proposition 3.1.19. Due to the fundamental property of prolongation (3.1) we have $j^r_Z(p) = g \cdot j^r_X(q)$. This implies $p = g \cdot q \in Z$ and $j^r_Z(p) = j^r_X(p)$. We verified that X and Z satisfy all conditions of Lemma 3.1.21. Then $X = Z = \overline{g \cdot X}$ and, therefore $g \in \mathrm{Sym}(X, G)$. □

Lemma 3.1.23. Suppose that X is a non-exceptional curve with respect to a classifying set of rational differential invariants $\mathcal{I} = \{K_1, K_2\}$. Then the following are equivalent:

(1) $K_1|_X$ is a constant function on X,

(2) $H = \mathrm{Sym}(X, G)$ is infinite,

(3) the signature $\mathcal{S}_X$ consists of a single point.

Proof. (1) $\Rightarrow$ (2) Assume $K_1|_X = c$ is a constant function on X. Fix a non-exceptional point p. We will show that any non-exceptional point on X belongs to the orbit Hp. Since non-exceptional points are dense in X, the conclusion would follow from Proposition 2.3.18.
Let q be a non-exceptional point on X. Then $K_1(j^k_X(p)) = K_1(j^k_X(q)) = c$ where k equals $\mathrm{ord}(K_1)$. Since K_1 is separating on J^k, there exists $g \in G$, such that $j^k_X(p) = g \cdot j^k_X(q)$. Consider a curve $Z = \overline{g \cdot X}$. By Lemma 3.1.17, Z is non-exceptional. Condition $\overline{\mathcal{S}}_X = \overline{\mathcal{S}}_Z$ holds due to Proposition 3.1.19. Therefore $K_1|_Z$ is the same constant function as $K_1|_X$. Due to the fundamental property of prolongation (3.1) we have $j^r_Z(p) = g \cdot j^r_X(q)$. This implies $p = g \cdot q \in Z$ and $j^r_Z(p) = j^r_X(p)$. We verified that X and Z satisfy all conditions of Lemma 3.1.20. Then $X = Z = \overline{g \cdot X}$ and, therefore $g \in H$ and so $q \in Hp$.
(2) $\Rightarrow$ (3) Let p be a non-exceptional point. For any $q \in Hp$, there exists $g \in H$, such that $p = g \cdot q$ and $X = g \cdot X$. If q is non-exceptional, it follows from (3.1) that $j^k_X(p) = g \cdot j^k_X(q)$. Since K_1 is a differential invariant, $K_1|_X(g \cdot j^k_X(q)) = K_1|_X(j^k_X(q))$. Then

$$K_1|_X(j^k_X(p)) = K_1|_X(j^k_X(q)) \text{ for all non-exceptional } q \in H_p.$$

Since H is infinite, from Proposition 2.3.18, it follows the orbit Hp is dense in X. The set of non-exceptional points is also dense in X. Thus $K_1|_X$ is a constant rational function on a dense subset of X and, therefore, is constant on X.
(3) $\Rightarrow$ (1) Obvious from the definition of $\mathcal{S}_X$. □

We are now ready to prove the converse of the Proposition 3.1.19.

Proposition 3.1.24. If algebraic curves $X, Y \subset \mathbb{C}^2$ are non-exceptional with respect to a classifying set of rational differential invariants $\mathcal{I} = \{K_1, K_2\}$ under an action of G on $\mathbb{C}^2$ and their signature curves are equal, $\overline{\mathcal{S}_X} = \overline{\mathcal{S}_Y}$, then X and Y are G-equivalent.

Proof. Then $\mathcal{S} := \overline{\mathcal{S}_X} = \overline{\mathcal{S}_Y}$ is an irreducible curve, and let $S(\kappa_1, \kappa_2)$ be its defining polynomial. If $\frac{\partial S}{\partial \kappa_2}$ were identically zero, then $K_1|_X$ would be constant and Lemma 3.1.23 would imply that $\mathcal{S}$ is a single point. Therefore $\frac{\partial S}{\partial \kappa_2}|_s$ is nonzero for all but finitely many points $s \in \mathcal{S}$. Moreover, since X and Y are non-exceptional, for all but finitely many such points $s \in \mathcal{S}$, none of the points in the preimage $\sigma_X^{-1}(s)$ are exceptional in X and none of the points in the preimage $\sigma_Y^{-1}(s)$ are exceptional in Y. By Chevalley's Theorem (2.2.27), the images $\mathcal{S}_X$ and $\mathcal{S}_Y$ are open subsets of $\mathcal{S}$, and thus all but at most finitely many points of $\mathcal{S}$. We fix a point $s \in \mathcal{S}$ with these desired properties, a point $p \in \sigma_X^{-1}(s)$ and a point $q \in \sigma_Y^{-1}(s)$. Otherwise $\overline{\mathcal{S}_X}$ (and, therefore, $\overline{\mathcal{S}_Y}$) is a single point, and we let p and q be any non-exceptional points on X and Y, respectively.

In both cases, $\sigma_X(p) = \sigma_Y(q)$, meaning that

$$K_1(j_X^r(p)) = K_1(j_Y^r(q)) \quad \text{and} \quad K_2(j_X^r(p)) = K_2(j_Y^r(q)).$$

Since $\mathcal{I}$ is separating and p and q are non-exceptional, there exists a group element $g \in G$ for which $j_X^r(p)$ equals $g \cdot j_Y^r(q)$.
Consider a curve $Z = \overline{g \cdot Y}$. By Lemma 3.1.17, Z is non-exceptional. Condition $\overline{\mathcal{S}_X} = \overline{\mathcal{S}_Z}$ holds due to Proposition 3.1.19. Due to the fundamental property of prolongation (3.1), we have $j_Z^r(p) = g \cdot j_X^r(q)$. Therefore, $p = g \cdot q \in Z$ and $j_Z^r(p) = j_X^r(p)$. We verified that X and Z satisfy all conditions of Lemma 3.1.21. Then $X = Z = \overline{g \cdot Y}$. □

Combining Lemma 3.1.23 with Propositions 3.1.19 and 3.1.24 we get the following corollary.

Corollary 3.1.25. If X and Y have a finite symmetry group, then X and Y are G-equivalent if and only if their signature polynomials S_X, S_Y are equal up to a non-zero constant factor.

We can now combine the results in this section to establish, for the action of each $G \subset \mathcal{PGL}(3)$, the existence of a pair of classifying invariants that characterize the equivalence classes of generic irreducible algebraic curves.

Theorem 3.1.26. Let r-dimensional group $G \subset \mathcal{PGL}(3)$ act on $\mathbb{C}^2$. Then there exists a pair of differential invariants $\mathcal{I} = \{K_1, K_2\}$ of differential order at most r, such that for all integers d, where $\binom{d+2}{2} - 2 \geq r$, there exists a Zariski open subset $\mathcal{P}_d \subset \mathbb{C}[x, y]_{\leq d}$ such that any curves X, Y whose defining polynomials lie in $\mathcal{P}_d$ satisfy:

$$X \underset{G}{\cong} Y \quad \Longleftrightarrow \quad \overline{\mathcal{S}_X} = \overline{\mathcal{S}_Y}, \tag{3.9}$$

where $\mathcal{S}_X$ and $\mathcal{S}_Y$ are signatures of X and Y based on invariants $\mathcal{I}$, as given by Definition 3.1.18.

Proof. From Theorem 3.1.11 we know that there exists a classifying set $\mathcal{I}$ of rational differential invariants of order at most r. By Propositions 3.1.19 and 3.1.24, the statement (3.9) is valid for all $\mathcal{I}$-non-exceptional curves. By Theorem 3.1.16, for any d, such that $\binom{d+2}{2} - 2 \geq r$, there exists a Zariski open subset $\mathcal{P}_d \subset \mathbb{C}[x, y]_{\leq d}$, such that all curves whose defining polynomials lie in $\mathcal{P}_d$ are non-exceptional. □

Analagous to a similar property observed in smooth curves [11], when $\mathrm{Sym}(X, G)$ is a finite subgroup of G of size n, a signature map on X is also *generically* $n:1$. This result will play a crucial role in Section 3.2, where we study the algebraic properties of the signature polynomial.

Theorem 3.1.27. Suppose that X is a non-exceptional curve with respect to a classifying set of rational differential invariants $\mathcal{I} = \{K_1, K_2\}$ for action G. Then $|\mathrm{Sym}(X, G)| = n$ if and only if the map σ_X is generically $n:1$.

Proof. ($\Rightarrow$) We need to show that there exists a dense subset $\mathcal{S}_0 \subset \overline{\mathcal{S}_X}$, such that $|\sigma_X^{-1}(s)| = n$ for all $s \in \mathcal{S}_0$. Denote $H := \mathrm{Sym}(X, G)$. Since H is finite, from Lemma 3.1.23, it follows that $\overline{\mathcal{S}_X}$ is an irreducible curve and its defining polynomial $S(\kappa_1, \kappa_2)$ depends non-trivially on κ_2. Therefore the set $\mathcal{S}_1 = \left\{ s \in \mathcal{S}_X \;\middle|\; \left.\frac{\partial S}{\partial \kappa_2}\right|_s \neq 0 \right\}$ is dense in $\overline{\mathcal{S}_X}$. Due to Proposition 2.3.19 for all but maybe finitely many points $p \in X$, the orbit Hp consists of exactly n distinct points. Moreover, since X has only finitely many exceptional points, the set of points

$$X_0 = \{p \in X \mid Hp \text{ consists of exactly } n \text{ non-exceptional points}\}$$

is dense in X. Then its image $\mathcal{S}_2 = \sigma_X(X_0)$ is dense in $\overline{\mathcal{S}_X}$. It follows that the intersection $\mathcal{S}_0 := \mathcal{S}_1 \cap \mathcal{S}_2$ is dense in $\overline{\mathcal{S}_X}$. For any $s \in \mathcal{S}_0$, let $p \in \sigma_X^{-1}(s)$. By Lemma 3.1.22, $\sigma_X^{-1}(s) = Hp$ and so $|\sigma_X^{-1}(s)| = n$.

($\Leftarrow$) Suppose that the map σ_X is generically $n:1$. Then, by Lemma 3.1.23, $\mathrm{Sym}(X, G)$ is finite. By the forward implication, $n = \mathrm{Sym}(X, G)$. □

Example 3.1.28. Consider the special Euclidean group $\mathcal{SE}(2)$ of complex translations and rotations of $\mathbb{C}^2$ (see Example 2.3.10). The set $\mathcal{I}^{\mathcal{SE}} = \{K_1, K_2\}$, where $K_1 = \kappa^2$, the square of Euclidean curvature, and $K_2 = \kappa_s$ its derivative with respect to Euclidean arc-length, is classifying (see Proposition 4.1.1). Indeed, one can check directly that $\mathcal{I}^{\mathcal{SE}}$ separates orbits on the $\mathcal{SE}$-invariant open subset

$$W_2 = \left\{ \left(x, y, y^{(1)}, y^{(2)}, y^{(3)}\right) \mid \left(y^{(1)}\right)^2 + 1 \neq 0 \right\}$$

and K_1 separates orbits on an open set $W_1 = \pi(W_2) \subset J^2$ under the standard projection $\pi\colon J^3 \to J^2$. Thus the conditions of Definition 3.1.6 are satisfied. According to Theorem 3.1.11 we conclude that

$$\mathbb{C}(J^3)^{\mathcal{SE}(2)} = \mathbb{C}(K_1, K_2) \quad \text{and} \quad \mathbb{C}(J^2)^{\mathcal{SE}(2)} = \mathbb{C}(K_1).$$

By Theorem 3.1.16, a generic curve of degree ≥ 2 is non-exceptional with respect to $\mathcal{I}^{\mathcal{SE}}$. In fact, a careful consideration of the conditions in Definition 3.1.13 shows that there are *no* irreducible curves of degree greater than one that are $\mathcal{I}^{\mathcal{SE}}$-exceptional.

We will now compute the signature polynomial for the ellipse X defined by the zero set of

$$F(x, y) = x^2 + y^2 + xy - 1.$$

The signature map $\sigma_X = (K_1|_X, K_2|_X) : X \to \mathbb{C}^2$ is explicitly defined by

$$K_1|_X(x,y) = 36\frac{(x^2+xy+y^2)^2}{(5x^2+8xy+5y^2)^3} \quad \text{and} \quad K_2|_X(x,y) = 54\frac{(y^4-x^4+xy^3-x^3y)}{(5x^2+xy+y^2)^3}.$$

Under the $\mathcal{SE}(2)$-action the ellipse has a symmetry group of cardinality two generated by the 180°-degree rotation. We observe that in agreement with Theorem 3.1.27, σ_X is generically a $2\colon 1$ map on X. One can use a Gröbner basis elimination algorithm to compute a signature polynomial of X, that is an irreducible polynomial vanishing on the image of rational map σ_X:

$$S_X(\kappa_1,\kappa_2) = 2916\kappa_1^6 + 972\kappa_1^4\kappa_2^2 + 108\kappa_1^2\kappa_2^4 + 4\kappa_2^6 - 13608\kappa_1^5 + 1944\kappa_1^3\kappa_2^2 + 2187\kappa_1^4.$$

Any curve $\mathcal{SE}(2)$-equivalent to X will have the same signature polynomial. For most degree three algebraic curves, it takes much longer to compute their signature polynomials under $\mathcal{SE}(2)$ actions, and for higher degree curves it is rarely possible in practice. For this reason, it is of interest to determine properties, such as the degree, of signature polynomials for curves without their explicit computation, which we discuss in Section 3.2.

3.2 Properties of signature polynomials

In Section 3.1.1 we showed the existence of signature map, whose image characterized equivalence classes of generic irreducible algebraic curves. The closure of this image, the signature curve, is defined by an irreducible polynomial called the signature polynomial. In this section we explore properties of signature polynomials and signature curves. For the action of $G \subset \mathcal{PGL}(3)$ we fix a classifying pair of differential invariants $\mathcal{I} = \{K_1, K_2\}$, and we denote the signature map defined by $\mathcal{I}$ restricted to an algebraic curve $X \subset \mathbb{C}^2$ as σ_X.

3.2.1 Degree of signature polynomials

In Section 2.2.3 we considered the image of a rational map on an irreducible projective curve in $\mathbb{CP}^2$ and showed how one can determine the degree of the irreducible polynomial vanishing on this image. To use these results, for a signature map $\sigma_X : X \dashrightarrow \mathbb{C}^2$, non-constant on X, we consider a projective extension (see Definition 2.2.22) $\boldsymbol{\sigma} : \mathbb{CP}^2 \dashrightarrow \mathbb{CP}^2$. Note that while we will drop X from the notation, the map $\boldsymbol{\sigma}$ still heavily depends on the original curve X.

Theorem 3.2.1. Let $X \subset \mathbb{C}^2$ be a non-exceptional algebraic curve defined by an irreducible polynomial F, and let $n = |\operatorname{Sym}(X,G)|$. Then for any homogeneous vector $\boldsymbol{\sigma}$, defining a projective extension $\boldsymbol{\sigma} : \mathbb{CP}^2 \dashrightarrow \mathbb{CP}^2$ of the signature map σ_X, the degree of the signature

polynomial S_X satisfies

$$n \cdot \deg(S_X) \quad = \quad \deg(\mathbf{F}) \cdot \deg(\boldsymbol{\sigma}) - \sum_{\mathbf{p} \in Bl(\boldsymbol{\sigma})} \operatorname{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\sigma}). \tag{3.10}$$

Here $\mathbf{F} \in \mathbb{C}[x_0, x_1, x_2]$ denotes the homogenization of F.

Proof. From Theorem 3.1.27 we know that $\sigma_X : X \dashrightarrow \mathbb{C}^2$ is generically $n:1$ map. Then $\boldsymbol{\sigma}$ is defined and generically $n:1$ on $V(\mathbf{F})$, which is the Zariski-closure of X in $\mathbb{CP}^2$. Since F, and thus $\mathbf{F}$, is irreducible, the minimal polynomial $\mathbf{P}$ vanishing on the image $\boldsymbol{\sigma}(V(\mathbf{F}))$ is also irreducible. Its dehomogenezation is exactly the signature polynomial S_X. The result then follows from Theorem 2.2.52. □

Theorem 3.2.2. Let $X \subset \mathbb{C}^2$ be a non-exceptional algebraic curve defined by an irreducible polynomial F, and let $n = |\operatorname{Sym}(X, G)|$. For any homogeneous vector $\boldsymbol{\sigma}$, defining a projective extension $\boldsymbol{\sigma} : \mathbb{CP}^2 \dashrightarrow \mathbb{CP}^2$ of the signature map σ_X, denote $\boldsymbol{\sigma}^0$ as the vector $[\boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2]$ and $\boldsymbol{\sigma}^1, \boldsymbol{\sigma}^2$ similarly. Then the degree of the signature polynomial $S_X \in \mathbb{C}[\kappa_0, \kappa_1, \kappa_2]$ in each variable κ_i satisfies

$$n \cdot \deg_{\kappa_i}(S_X) \quad = \quad \deg(\mathbf{F}) \cdot \deg(\boldsymbol{\sigma}) - \sum_{\mathbf{p} \in Bl(\boldsymbol{\sigma}^i)} \operatorname{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\sigma}^i). \tag{3.11}$$

Here $\mathbf{F} \in \mathbb{C}[x_0, x_1, x_2]$ denotes the homogenization of F.

Proof. Similarly as in the proof of Theorem 3.2.1, the result follows from Theorem 2.2.53. □

In each case, the last term of (3.10) and (3.11) appears to be difficult to obtain, as we recall from Remark 2.2.47, for a vector of homogeneous polynomials $\boldsymbol{\phi}$, $\operatorname{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\phi})$ is defined as the minimal multiplicity over $\mathbf{a} \in \mathbb{CP}^2$. However, from Proposition 2.2.48, we can compute bounds for the multiplicities, and thus bounds for the degree of the signature polynomial. Moreover, for a generic choice of $\mathbf{a} \in \mathbb{CP}^2$, the upper bound is tight, giving a randomized algorithm to compute this degree.

Corollary 3.2.3. Under the hypotheses of Theorem 3.2.2, for any $\mathbf{a} \in \mathbb{CP}^2$ and $\mathbf{b} \in \mathbb{CP}^1$, we have

$$n \cdot \deg(S_X) \;\geq\; \deg(\mathbf{F}) \cdot \deg(\boldsymbol{\sigma}) - \sum_{\mathbf{p} \in Bl(\boldsymbol{\sigma})} m_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\sigma}^*_{\mathbf{a}}), \tag{3.12}$$

$$n \cdot \deg_{\kappa_i}(S_X) \;\geq\; \deg(\mathbf{F}) \cdot \deg(\boldsymbol{\sigma}^i) - \sum_{\mathbf{p} \in Bl(\boldsymbol{\sigma}^i)} m_{\mathbf{p}}(\mathbf{F}, (\boldsymbol{\sigma}^i)^*_{\mathbf{b}}) \tag{3.13}$$

with equality holding for a generic $\mathbf{a}$ and $\mathbf{b}$. In addition:

$$n \cdot \deg(S_X) \;\leq\; \deg(\mathbf{F}) \cdot \deg(\boldsymbol{\sigma}) - \sum_{\mathbf{p} \in Bl(\boldsymbol{\sigma})} m_{\mathbf{p}}(\langle \mathbf{F}, \boldsymbol{\sigma}_0, \boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2 \rangle), \tag{3.14}$$

$$n \cdot \deg_{\kappa_i}(S_X) \;\leq\; \deg(\mathbf{F}) \cdot \deg(\boldsymbol{\sigma}^i) - \sum_{\mathbf{p} \in Bl(\boldsymbol{\sigma}^i)} m_{\mathbf{p}}(J^i) \tag{3.15}$$

where $J^0 = \langle F, \boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2 \rangle$ and J^1, J^2 are defined similarly.

Proof. This is a direct corollary of Proposition 2.2.48, Theorem 3.2.1, and Theorem 3.2.2. □

For more on computing signature polynomials and bounds of their degree see Appendix A.

3.2.2 Generic monomial support and genus

The existence of a signature map for a generic algebraic curve of sufficiently high degree leads to question, "What properties are shared by the signature curves or signature polynomials for a generic algebraic curve?" In this subsection, for the action of a group G where $\dim(G) = r$, we assume that the degree d of an algebraic curve satisfies $\binom{d+2}{2} - 2 \geq r$. This ensures the existence of a non-empty open subset of $\mathbb{C}[x, y]_{\leq d}$ for each d where the signature map characterizes equivalence classes.

From Proposition 2.3.20 and Lemma 3.1.23 we can immediately see that for a generic curve X, where $\deg(X) \geq 3$, $\dim(\overline{\mathcal{S}}_X) = 1$. Thus a signature polynomial can be associated with a generic curve.

The *genus* of a smooth curve X, denoted $\chi(X)$ is determined by $d = \deg(X)$. It is given by the well-known genus-degree formula $\chi(X) = \frac{(d-1)(d-2)}{2}$ [23].

Each singularity of X reduces $\chi(X)$. For any choice of classifying invariants, we show below in Theorem 3.2.4 that the signature map preserves the genus of a generic curve. In Chapter 4 we investigate the degree of the signature polynomial of X under certain subgroups of $\mathcal{PGL}(3)$ and show that $\deg(S_X)$ is often much higher than $\deg(X)$. Thus, in these cases, $\chi(\overline{\mathcal{S}}) = \chi(X)$ implies that $\overline{\mathcal{S}}$ is a highly singular curve.

Theorem 3.2.4. A generic curve X of fixed degree $d \geq 4$, is birationally equivalent to its signature curve $\overline{\mathcal{S}}_X$. In this case the genus of $\overline{\mathcal{S}}_X$ is equal to the genus of X, i.e.

$$\chi(\overline{\mathcal{S}}_X) = \chi(X). \tag{3.16}$$

Proof. By Theorem 3.1.27 and Proposition 2.3.20, the signature map σ_X is generically one to one, which implies that σ_X is birational (see [51, pg. 99]). Then (3.16) follows from the fact that birationally equivalent curves have the same genus. □

Remark 3.2.5. Since a generic curve is smooth, the genus-degree formula $\frac{(d-1)(d-2)}{2}$ also gives the genus of the signature curve $\overline{\mathcal{S}}_X$ for generic X of degree d.

The signature polynomials of generic curves also have the same *monomial support*, which further implies that the polynomials have the same degree. This "generic degree" provides an upper bound for the degree of the signature polynomial for any non-exceptional curve with finite symmetry group.

Definition 3.2.6. Given a curve $X = V(F)$ defined by $F = \sum_{i,j} a_{ij}x^i y^j$ where $1 \leq i, j \leq d$, the **monomial support** of F is the set of points in $\mathbb{R}^2$ given by $\mathcal{M} = \{(i,j) \,|\, a_{ij} \neq 0\}$. The convex hull of $\mathcal{M}$ is the **Newton polytope** of F.

Theorem 3.2.7. For a generic curve X of fixed degree $d \geq 3$, the signature polynomials S_X have the same monomial support. In particular, the signature polynomials have the same degree and Newton polytope.

Proof. Let $\mathbf{a}$ denote the point $[a_{00} : a_{10} : \ldots : a_{0d}] \in \mathbb{CP}^N$ where $N = \binom{d+2}{2} - 1$, and consider the polynomial $F(x, y, \mathbf{a}) = \sum_{i,j} a_{ij}x^i y^j$ where $0 \leq i, j \leq d$. For a particular value $\tilde{\mathbf{a}} \in \mathbb{CP}^N$, $F_{\tilde{\mathbf{a}}} = F|_{\mathbf{a}=\tilde{\mathbf{a}}}$ defines a curve $V(F_{\tilde{\mathbf{a}}}) = X_{\tilde{\mathbf{a}}}$. For a generic choice of $\tilde{\mathbf{a}}$, this is an irreducible, non-exceptional curve of degree d by Theorem 3.1.16.

The rational map j^n_X induces a map $j^n : \mathbb{CP}^N \times \mathbb{C}^2 \dashrightarrow \mathbb{C}^{n+2}$ defined by the rational functions of the partials of F as in Remark 3.1.1. For a differential function K let $K|_F = K \circ j^n$ denote the restriction of K to an arbitrary curve of degree d. Consider the rational map $\sigma : \mathbb{CP}^N \times \mathbb{C}^2 \dashrightarrow \mathbb{CP}^N \times \mathbb{C}^2$ defined by $\sigma = (\mathbf{a}, K_1|_F, K_2|_F)$.

Since F is irreducible over $\mathbb{C}[x, y, \mathbf{a}]$, there exists an irreducible polynomial $P \in \mathbb{C}[\kappa_1, \kappa_2, \mathbf{a}]$ vanishing on the image of $V(F)$ under σ. By Chevalley's Theorem, this image is an open dense subset of $V(P)$, i.e. there exists a variety $\mathcal{H} \subset V(P)$ such that $\sigma(V(F)) \supset V(P) \backslash \mathcal{H}$ and $\dim(\mathcal{H}) \leq N$.

Consider the regular projection map $\pi : V(P) \to \mathbb{C}^N$ given by $\pi(\mathbf{a}, \kappa_1, \kappa_2) = \mathbf{a}$. We claim that $\dim(\pi^{-1}(\mathbf{a}) \cap \mathcal{H}) \leq 0$ for a generic $\mathbf{a}$. Suppose $\overline{\pi(\mathcal{H})} = \mathbb{C}^N$; otherwise for a generic $\mathbf{a}$, $\pi^{-1}(\mathbf{a}) \cap \mathcal{H}$ is empty. Then, for a generic choice of $\mathbf{a}$, the dimension of $\pi^{-1}(\mathbf{a}) \cap \mathcal{H}$ is given by $\dim(\mathcal{H}) - N$, meaning $\dim(\pi^{-1}(\mathbf{a}) \cap \mathcal{H}) \leq 0$ [50, Ch. 1, Sec 6.3, Theorem 7].

Suppose we take a generic point $\tilde{\mathbf{a}}$. Then there exists an irreducible signature polynomial $S_{X_{\tilde{\mathbf{a}}}}$ such that $V(S_{X_{\tilde{\mathbf{a}}}}) \subset V(P_{\tilde{\mathbf{a}}})$ where $P_{\tilde{\mathbf{a}}} = P(\kappa_1, \kappa_2, \mathbf{a})|_{\mathbf{a}=\tilde{\mathbf{a}}}$. If $P_{\tilde{\mathbf{a}}}$ is reducible then $P_{\tilde{\mathbf{a}}} = S_{X_{\tilde{\mathbf{a}}}}(\kappa_1, \kappa_2)H_{\tilde{\mathbf{a}}}(\kappa_1, \kappa_2)$. By genericity, points of the form $(\tilde{\mathbf{a}}, p)$ where $p \in V(H_{\tilde{\mathbf{a}}})$ necessarily lie outside the image of σ, meaning $(\tilde{\mathbf{a}}, p) \in \pi^{-1}(\tilde{\mathbf{a}}) \cap \mathcal{H}$. However, $\dim(\pi^{-1}(\tilde{\mathbf{a}}) \cap \mathcal{H}) \leq 0$, and hence there can only be finitely many points $p \in V(H_{\tilde{\mathbf{a}}})$ which contradicts the fact that $P_{\tilde{\mathbf{a}}}$ is reducible.

Therefore the polynomial $P_{\mathbf{a}}$ is irreducible for a generic value of $\mathbf{a}$, implying $S_{X_{\mathbf{a}}} = P_{\mathbf{a}}$. In this case the monomial support of $S_{X_{\mathbf{a}}}$ equals the monomial support of $P_{\mathbf{a}}$. We can write

$P = \sum_{i,j} b_{ij}\kappa_1^i\kappa_2^j$ where $1 \leq i, j \leq D = \deg_{\kappa_1,\kappa_2}(P)$ and $b_{ij} \in \mathbb{C}[\mathbf{a}]$. The point (i, j) being in the monomial support of $P_{\mathbf{a}}$ is equivalent to the condition that $b_{ij}(\mathbf{a}) \neq 0$, and hence is an open condition on $\mathbf{a}$. □

Theorem 3.2.8. Suppose that X is a curve of degree less than or equal to d (where $d \geq 4$) non-exceptional with respect to the classifying set $\mathcal{I}$ and with finite symmetry group. Then $\deg(S_X) \leq s_d$ where s_d is the degree of the signature curve for a generic curve of degree d.

Proof. For each $\binom{d+2}{2} - 2 \geq r$ where $r = \dim(G)$, the existence of s_d is proved in Theorem 3.2.7. Let $X = V(F)$ be any non-exceptional curve of degree $\leq d$ with finite symmetry group and H be a generic choice of polynomial in $\mathbb{C}[x, y]_{\leq d}$; consider the pencil defined by $F + \lambda H$. Since a generic curve is non-exceptional with finite symmetry group (Theorem 3.1.16), for all but finitely many values of $\lambda_0 \in \mathbb{C}$, $F + \lambda_0 H$ is an irreducible non-exceptional curve with finite symmetry group. One can check that $F + \lambda H$ is irreducible over $\mathbb{C}[x, y, \lambda]$.

Similarly as in the proof of Theorem 3.2.7, let $\sigma : \mathbb{C}^3 \dashrightarrow \mathbb{C}^3$ be the map defined by $\sigma = (K_1|_{F+\lambda H}, K_2|_{F+\lambda H}, \lambda)$, defined for all but perhaps finitely many values of λ. Denote the irreducible polynomial vanishing on the image $\sigma(V(F + \lambda H))$ as $P \in \mathbb{C}[\kappa_1, \kappa_2, \lambda]$. Then, for any value of λ_0 where $F + \lambda_0 H$ is non-exceptional, $\mathcal{S}_{V(F+\lambda_0 H)} \subset V(P|_{\lambda=\lambda_0})$.

For a generic choice of λ, the polynomial $P|_{\lambda=\lambda_0}$ is of degree s_d (by a similar argument as in Theorem 3.2.7). Since P is irreducible it does not contain the plane $\lambda = 0$, and hence the signature polynomial S_X is a factor of $P|_{\lambda=\lambda_0}$. In particular it is of degree less than or equal to s_d. □

If one considers the set of curves X of degree d under G, then the above results restrict the possible curves that can arise as signature curves for X. This could aide in developing different methods to compute or approximate the signature polynomial as discussed in Section 5.4.

Note, however, that the generic monomial support and upper bound on the degree of S_X depend on the set of classifying invariants. Using a different classifying pair of invariants may result in a different generic degree for S_X. The relationship between different classifying pairs of invariants is discussed in Section 5.2.

3.2.3 Real signature curves

For any algebraic curve $X = V(F)$, we can consider the zero set of F over $\mathbb{R}$ denoted $V_{\mathbb{R}}(F)$. When this is non-empty, there is an associated *real* algebraic curve $X_{\mathbb{R}} = V_{\mathbb{R}}(F)$ given by the real points of X. With any real algebraic curve $X_{\mathbb{R}} = V_{\mathbb{R}}(F)$, we can always consider the corresponding algebraic curve in $\mathbb{C}^2$ given by $X = V(F)$. Similarly there is a correspondence between an algebraic group $G \subset \mathcal{PGL}(3, \mathbb{C})$ and the subgroup $G_{\mathbb{R}} \subset \mathcal{PGL}(3, \mathbb{R})$ corresponding to

real elements of G. In this section we discuss the relationship between the signatures of algebraic curves X and the real part of X.

Suppose that $G_{\mathbb{R}} \subset \mathcal{PGL}(3,\mathbb{R})$ acts on $\mathbb{R}^2$ as defined in (2.10). In [10] the authors showed that a classifying pair of rational differential invariants defined a signature map, whose image characterized equivalence classes for non-exceptional real algebraic curves under this action. The terms "classifying"' and "non-exceptional" are defined as they are in this thesis, but over the real numbers.

Suppose a set of rational differential invariants $\mathcal{I} = \{K_1, K_2\}$ is classifying for both the action of $G_{\mathbb{R}}$ on $\mathbb{R}^2$ and G on $\mathbb{C}^2$. Since the curves X and $X_{\mathbb{R}}$ are defined by the same polynomial F, the rational map defined by $\sigma_X = (K_1|_X, K_2|_X)$ is the signature map for both X and $X_{\mathbb{R}}$. The real part of the image $\mathcal{S}_X$ contains the signature of $X_{\mathbb{R}}$. Thus, when $\mathrm{Sym}(X,G)$ is finite and $\dim(X_{\mathbb{R}}) = 1$, the minimal polynomial vanishing on the signature of $X_{\mathbb{R}}$ is the signature polynomial S_X.

This shows that even if one is only concerned with real algebraic curves, the results derived here for signature polynomials of curves $X \subset \mathbb{C}^2$ are relevant. However, there are some differences: in the case of complex curves, the Zariski closure of the signature and thus the signature polynomial characterizes equivalence classes of X under G, while the equivalence classes of real curves $X_{\mathbb{R}}$ under $G_{\mathbb{R}}$ are characterized by their image under σ_X. In fact, two real curves $X_{\mathbb{R}}$ and $Y_{\mathbb{R}}$ may have the same signature polynomial $S := S_X = S_Y$, but different images under σ_X and hence different signatures (see Example 3.2.12).

In [10] the authors provided examples of classifying pairs of invariants for $\mathcal{A}(2,\mathbb{R})$, and $\mathcal{PGL}(3,\mathbb{R})$. In Section 4.1.1 we show that these same invariants are also classifying for $\mathcal{A}(2,\mathbb{C})$, and $\mathcal{PGL}(3,\mathbb{C})$ respectively. An interesting question is whether the existence of a classifying pair of invariants for the action of $G_{\mathbb{R}}$ is guaranteed, i.e. a similar statement to Theorem 3.1.11 is true over the real numbers.

Remark 3.2.9. Many properties of the field of rational invariants that were integral to the proof of Theorem 3.1.11 no longer hold when the ground field is $\mathbb{R}$. For instance, the second part of Proposition 2.3.8 is not true over $\mathbb{R}$.

For example, the field of rational invariants for the action of the group $\mathbb{R}^*$ (non-zero real numbers under multiplication) on $\mathbb{R}^2$ defined by $(x,y) \mapsto (\lambda^2 x, \lambda^2 y)$ is generated by $K = \frac{x}{y}$, but K is not separating. Conversely, for the translation action of $\mathbb{R}$ on $\mathbb{R}^2$ defined by $(x,y) \mapsto (x+a, y)$, the invariant $K = y^3$ is separating but not generating.

The invariant $K = \frac{x}{y}$ also generates the ring of invariants for the action of $\mathbb{C}^*$ on $\mathbb{C}^2$ defined by $(x,y) \mapsto (\lambda^2 x, \lambda^2 y)$. Therefore this invariant is separating for this action, but not for the associated action of $\mathbb{R}^*$ on $\mathbb{R}^2$. Conversely, for the translation action of $\mathbb{R}$ on $\mathbb{R}^2$ defined by $(x,y) \mapsto (x+a, y)$, the invariant $K = y^3$ is separating but not generating. Thus it is not

generating for the associated action of $\mathbb{C}$ on $\mathbb{C}^2$, meaning it cannot separate orbits for this action.

A more ambitious goal would be to establish the existence of a single classifying pair of rational differential invariants for *both* G and $G_{\mathbb{R}}$. As seen in the previous remark, invariants may separate orbits of $G_{\mathbb{R}}$, but not the orbits of G and vice versa.

3.2.4 Examples

In this section, we present some examples, illustrating the degree formula (3.10), the bounds we established in Corollary 3.2.3, as well as other properties of signature polynomials. We use pairs of classifying invariants introduced in Section 4.1. The algorithms used to compute the signature polynomial, degree bounds for the signature polynomial, and other quantities are detailed in Appendix A.

Example 3.2.10. Consider the curve X defined by the zero set of the irreducible cubic

$$F(x, y) = x^2y + y^2 + y + \frac{64}{121}$$

under the action of the affine group $\mathcal{A}(2)$ on $\mathbb{C}^2$. If we restrict the classifying invariants to X and cancel common factors, then we can construct a projective extension $\boldsymbol{\sigma}$ of σ_X where $\deg(\boldsymbol{\sigma}) = 26$.

In Figure 3.1 in red, on the left, the real affine points of X are shown, while on the right, the real affine points of its signature curve $\overline{\mathcal{S}_X}$. In blue, on the right, is the line $V(\mathbf{L})$ defined by $\mathbf{a} = [5 : 1 : 1]$ and on the left its pullback $V(\boldsymbol{\sigma}^*_{\mathbf{a}})$. Under the action of the affine group of transformations on the plane, X has a symmetry group of size two. Then by Theorem 3.1.27, the map $\boldsymbol{\sigma}$ is generically $2\colon 1$ on X.
A direct computation of the rightmost terms in (3.12) and (3.14) give that

$$\sum_{\mathbf{p}\in Bl(\boldsymbol{\sigma})} m_{\mathbf{p}}(\mathbf{F}, 5\boldsymbol{\sigma}_0 + \boldsymbol{\sigma}_1 + \boldsymbol{\sigma}_2) = \sum_{\mathbf{p}\in Bl(\boldsymbol{\sigma})} m_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\sigma}_0, \boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2) = 30$$

This allows us to conclude that $\sum_{\mathbf{p}\in Bl(\boldsymbol{\sigma})} \operatorname{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\sigma}) = 30$. Thus by Theorem 3.2.1 the degree of the signature curve equals $\deg(S_X) = (3 \cdot 26 - 30)/2 = 24$.

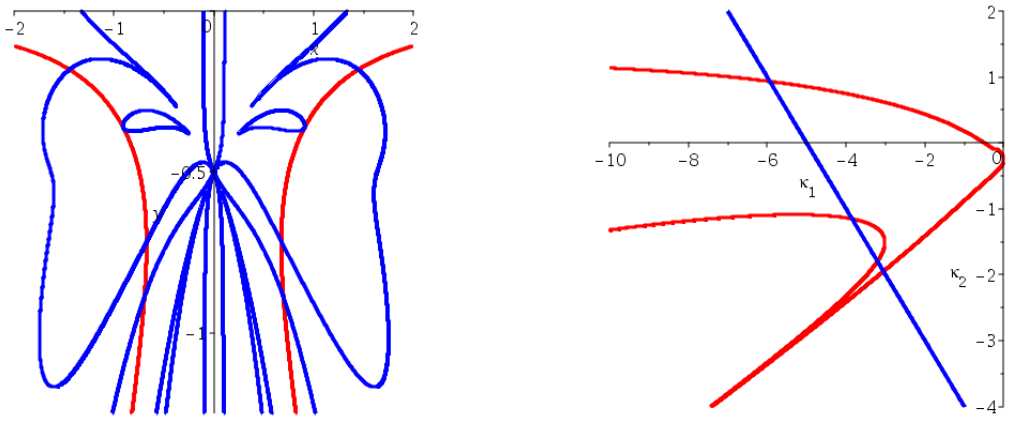

Figure 3.1: X and $\overline{\mathcal{S}_X}$ intersected with $V(\boldsymbol{\sigma}^*_{\mathbf{a}})$ and $V(\mathbf{L})$ respectively.

We now show that a line $\tilde{\mathbf{L}}$ defined by $\tilde{\mathbf{a}} = [1 : -6 : 1]$ does not provide us with exact degree count (the corresponding pictures are given by Figure 3.2). For this choice of line, $\sum_{\mathbf{p}\in Bl(\boldsymbol{\sigma})} m_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\sigma}_0 - 6\boldsymbol{\sigma}_1 + \boldsymbol{\sigma}_2) = 32$ and Corollary 3.2.3 tells us only that $23 \leq \deg(S_X) \leq 24$ and that $\tilde{\mathbf{a}}$ is non-generic. Indeed, $V(\tilde{\mathbf{L}})$ intersects $\overline{\mathcal{S}_X}$ at the point $[0 : 6 : 1]$ which is not in $\mathcal{S}_X$, a property that must be avoided by generic lines.

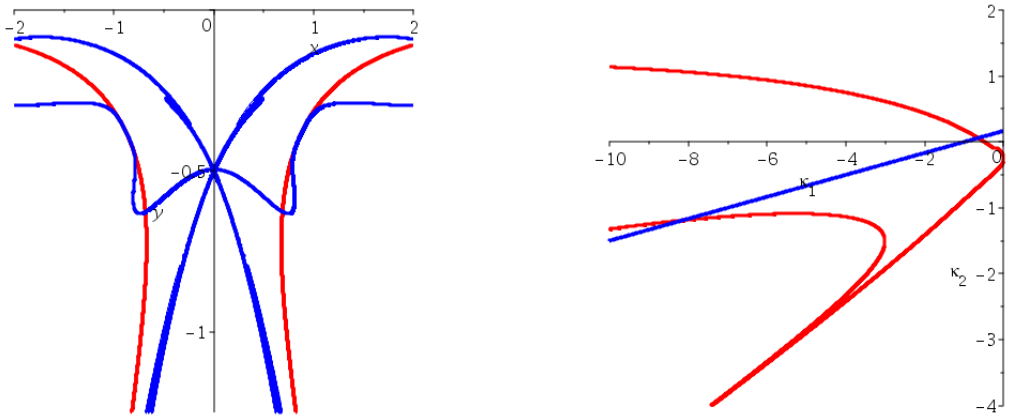

Figure 3.2: X and $\overline{\mathcal{S}_X}$ intersected with with $V(\boldsymbol{\sigma}^*_{\tilde{\mathbf{a}}})$ and $V(\tilde{\mathbf{L}})$ respectively.

Example 3.2.11. Let X denote the curve defined by the zero set of the elliptic curve

$$F(x, y) = y^2 - x(x + 1)(x + 2),$$

and consider X under the action of the special Euclidean group $\mathcal{SE}(2)$. A direct computation of the rightmost terms in (3.12) and (3.14) using $\mathbf{a} = [-7 : 5 : 3]$ give that $24 \leq \deg(S_X) \leq 24$. One can compute the signature polynomial directly to verify this.

The length of this signature polynomial illustrates how the signature polynomial, even for a simple elliptic curve, can be quite complicated. In fact, a first attempt at graphing the real affine points of $V(S_X)$ in Maple yields the "Snowman-like" figure:

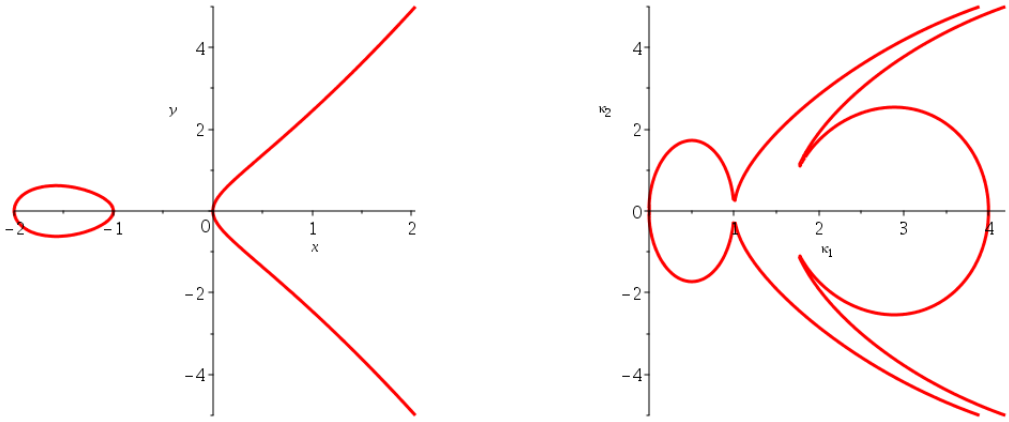

Figure 3.3: The elliptic curve X and a plot of $V(S_X)$.

However, this figure is misleading; the plotter in Maple has difficulty plotting around the singular points of $V(S_X)$ on the x-axis. To obtain a more accurate representation of the real affine points of $V(S_X)$, we can use bertini_real, a software that numerically decomposes and visualizes the real part of algebraic curves and surfaces [8].

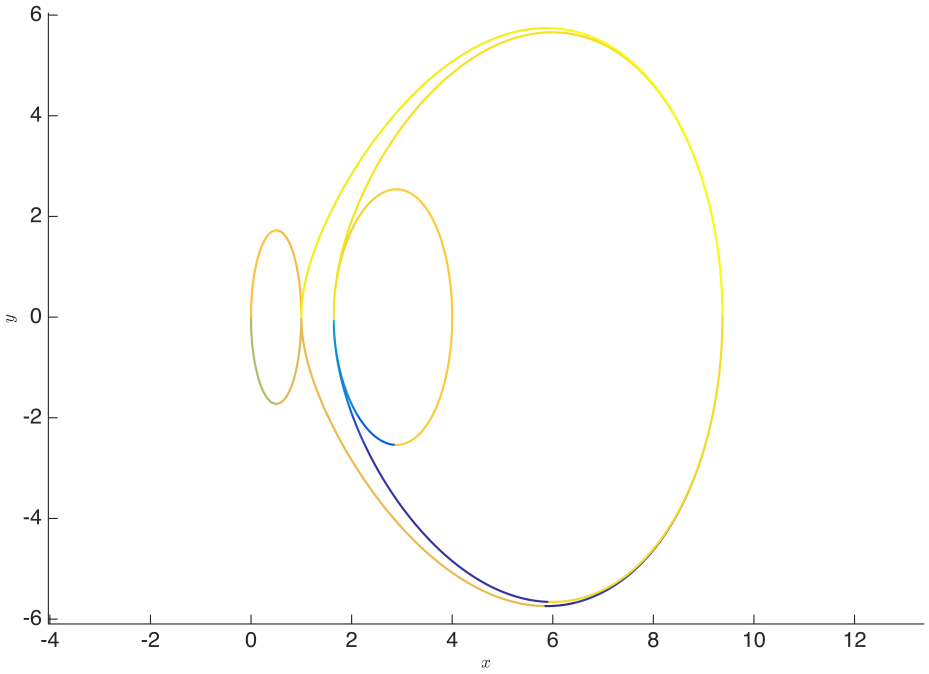

Figure 3.4: The real affine points of $V(S_X)$ in bertini_ real.

The software also allows us to zoom in closer to interesting parts of the curve. In Figure 3.5, the blue dots represent critical points of the curve. Note that there are four isolated points of $V(S_X)$. In particular, the two points to the left of the y-axis are the image of complex points of X.

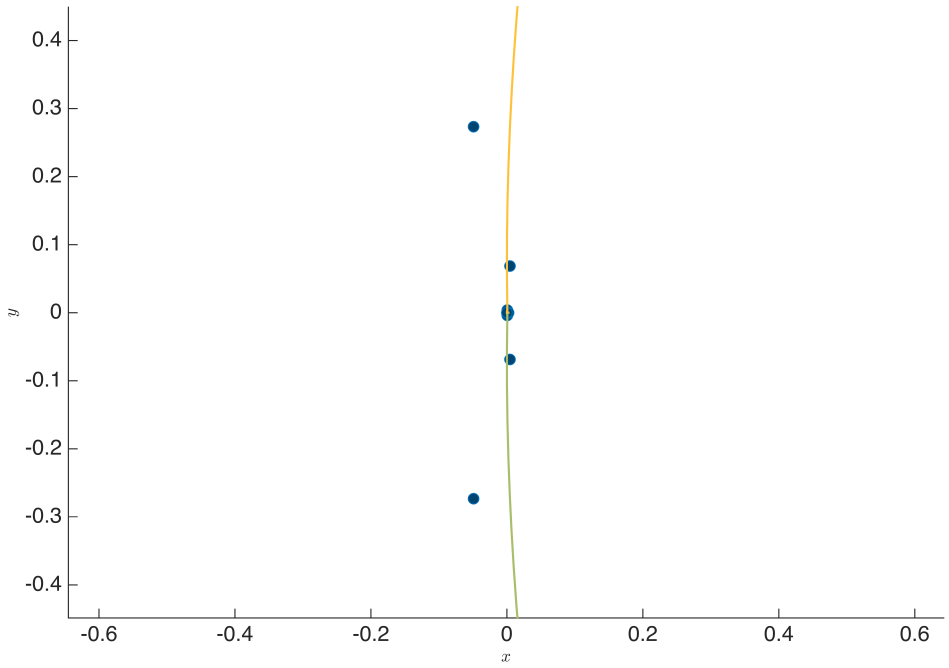

Figure 3.5: A closer look around the origin.

Observations seem to indicate that two similar isolated critical points appear in most cubic's Euclidean signature. An interesting question is whether these two points have any geometric significance. In Figure 3.6, we see that there exists a very small oval near the origin.

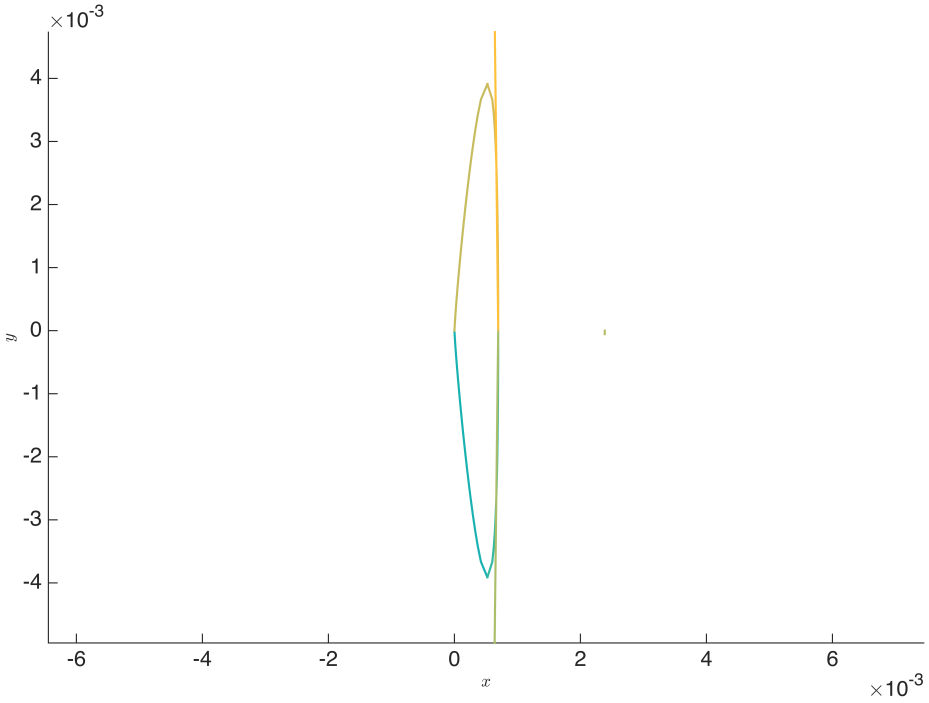

Figure 3.6: An even closer look around the origin.

From the above figures, we can see that the signature polynomial has a high degree of singularity.

Example 3.2.12. Consider the two cubics

$$F_1(x, y) = x^3 - y^2 + 1$$
$$F_2(x, y) = x^3 - y^2 - 1$$

under the action of the affine group $\mathcal{A}(2)$. These two curves have the same signature polynomial, and hence are $Af(2)$-equivalent by Proposition 3.1.24. However, one can verify directly that these curves are **not** $\mathcal{A}(2, \mathbb{R})$-equivalent. Thus the real part of the images of σ_{X_1} and σ_{X_2} correspond to different subsets of $V(S_{X_1})_{\mathbb{R}} = V(S_{X_2})_{\mathbb{R}}$.

Example 3.2.13. Prior knowledge of the degree of a signature polynomial can distinguish inequivalent curves. Consider the two quintics

$$F_1(x,y) = x^5 + xy + x - y + 1$$
$$F_2(x,y) = (x+2y)^5 + y^3 + y^2 + x^2 + x + 1$$

under the action of the affine group $\mathcal{A}(2)$. At first one might compute the size of the two curves' symmetry groups under $\mathbb{A}(2)$, as two curves X_1 and X_2 are $\mathcal{A}(2)$-equivalent if and only if $|\operatorname{Sym}(X_1, \mathcal{A}(2))| = |\operatorname{Sym}(X_2, \mathbb{A}(2))|$. However, in this case, both symmetry groups are trivial, yielding no new information.

Using $\mathbf{a} = [1:1:1]$ to compute the bounds (3.12) and (3.14) give that

$$30 \leq \deg(S_{X_1}) \leq 35$$
$$216 \leq \deg(S_{X_1}) \leq 216,$$

implying that the curves cannot have the same signature polynomial, and hence are inequivalent under $\mathcal{A}(2)$. Note that the degrees of both signature polynomials are quite large, indicating that direct computation using Gröbner basis algorithms would be difficult.

Example 3.2.14. Consider the class of plane curves defined by the zero set of

$$F(x,y) = y^2 - f(x)$$

where $f(x)$ is a univariate polynomial of degree > 4. In the case that $f(x)$ is a polynomial with no multiple roots and $\deg(f)$ is odd, $X = V(F)$ is known as a *hyperelliptic curve* [50]. The restrictions of the classifying invariants for the projective $\mathcal{PGL}(3)$ and affine $\mathcal{A}(2)$ actions yield projective extensions of the form $\boldsymbol{\sigma} = [\boldsymbol{\sigma}_0(y^2,x), \boldsymbol{\sigma}_1(y^2,x), \boldsymbol{\sigma}_2(y^2,x)]$. In fact each $\boldsymbol{\sigma}_i$ is a polynomial in y^2 and the partial derivatives of $f(x)$.

Therefore we can write the signature polynomial as the image of a rational map on $\mathbb{CP}^1$, implying that S_X is rational and the genus of S_X is $\chi(S_X) = 0$. When $\deg(f) = 2n+1$ for some integer $n \geq 2$, the genus of the curve is $\chi(X) = n$ [50]. This implies that there exists a class of curves with arbitrarily high genus, but rational signature polynomial. An interesting problem would be to use the degree formula (3.10) to investigate the degree of signature polynomials of hyperelliptic curves.

CHAPTER 4

Classical subgroups of the projective general linear group

In Chapter 4 we illustrate the results derived in Chapter 3 for the actions of the projective, affine, special affine, similarity, Euclidean, and special Euclidean groups on $\mathbb{C}^2$. We show that one can use classical differential invariants to build rational pairs of invariants and that these invariants are classifying. For the projective and affine actions, we use the same classifying invariants as in [10] for real algebraic curves.

For all of these groups we use the degree formula (3.10) to compute degree of the signature polynomial for a generic algebraic curve of fixed degree d. We do this by constructing projective extensions of the signature map for each group, and then computing each term in (3.10) for a generic curve. We conclude by examining the class of curves, known as Fermat curves, of the form $X = V(x^d + y^d + 1)$ for some positive integer $d \geq 2$. Under the projective and affine groups, we show that the degree of the signature polynomial remains constant for $d \geq 3$, and explicitly compute the signature polynomials for all Fermat curves of degree greater than three.

4.1 Classifying invariants

Here we introduce rational classifying pairs of invariants for the actions of $\mathcal{PGL}(3)$ and some of its well-known subgroups: the affine group $\mathcal{A}(2)$, the special affine group $\mathcal{SA}(2)$, the similarity group $\mathcal{S}(2)$, the Euclidean group $\mathcal{E}(2)$, and the special Euclidean group $\mathcal{SE}(2)$. For descriptions of each of these groups see Section 2.3.1; their actions on $\mathbb{CP}^2$ and $\mathbb{C}^2$ are given by (2.9) and (2.10).

In [10], the authors used classical differential invariants to build two lowest order rational

invariants for the projective and affine groups and directly proved that they satisfy conditions of Definition 3.1.6 for classifying invariants over $\mathbb{R}$ (see Theorem 4 in [10]). Using the same line of argument, we can show that these invariants are classifying over $\mathbb{C}$, and also produce classifying pairs for the actions of the special affine, Euclidean, and special Euclidean groups over $\mathbb{C}$. Additionally we provide a pair of classifying invariants for the action of the similarity group over $\mathbb{C}$.

The following inductive expressions [19, 40] for classical differential invariants are useful for expressing these pairs in a concise manner. We start with the classical Euclidean curvature and arc-length:

$$\kappa = \frac{y^{(2)}}{(1+[y^{(1)}]^2)^{3/2}}, \quad ds = \sqrt{1+[y^{(1)}]^2}dx. \tag{4.1}$$

We can then express the special affine curvature and arc-length in terms of them:

$$\mu = \frac{3\kappa(\kappa_{ss}+3\kappa^3)-5\kappa_s^2}{9\kappa^{8/3}}, \qquad d\alpha = \kappa^{1/3}ds,$$

where these expressions agree with the notion of special affine curvature and arc-length in Section 2.1.1. In a similar manner, the projective curvature and arc-length are

$$\eta = \frac{6\mu_{\alpha\alpha\alpha}\mu_\alpha - 7\mu_{\alpha\alpha}^2 - 9\mu_\alpha^2\mu}{6\mu_\alpha^{8/3}}, \qquad d\rho = \mu_\alpha^{1/3}d\alpha.$$

From these expressions we can construct the following pairs of invariants:

Group	$\mathcal{SE}(2)$	$\mathcal{E}(2)$	$\mathcal{S}(2)$	$\mathcal{SA}(2)$	$\mathcal{A}(2)$	$\mathcal{PGL}(3)$
K_1	κ^2	κ^2	$\frac{\kappa_s}{\kappa^2}$	μ^3	$\frac{\mu_\alpha^2}{\mu^3}$	η^3
K_2	κ_s	κ_s^2	$\frac{\kappa_{ss}}{\kappa^3}-3$	μ_α	$\frac{\mu_{\alpha\alpha}}{\mu^2}$	η_ρ

(4.2)

We can also express the invariants in terms of the jet coordinates. Refer to Table 4.1 for the explicit formulas of the Θ's.

Group	$\mathcal{SE}(2)$	$\mathcal{E}(2)$	$\mathcal{S}(2)$	$\mathcal{SA}(2)$	$\mathcal{A}(2)$	$\mathcal{PGL}(3)$
K_1	$\frac{(\Theta_2)^2}{(\Theta_1)^3}$	$\frac{(\Theta_2)^2}{(\Theta_1)^3}$	$\frac{\Theta_3}{(\Theta_2)^2}$	$\frac{(\Theta_4)^3}{(\Theta_2)^8}$	$\frac{(\Theta_5)^2}{(\Theta_4)^3}$	$\frac{(\Theta_7)^3}{(\Theta_5)^8}$
K_2	$\frac{\Theta_3}{(\Theta_1)^3}$	$\frac{(\Theta_3)^2}{(\Theta_1)^6}$	$\frac{\Theta_9}{(\Theta_2)^3}$	$\frac{\Theta_5}{(\Theta_2)^4}$	$\frac{\Theta_6}{(\Theta_4)^2}$	$\frac{\Theta_8}{(\Theta_5)^4}$

(4.3)

$$\Theta_1 = u_1^2 + 1 \qquad \Theta_2 = u_2 \qquad \Theta_3 = u_3\Theta_1 - 3u_1\Theta_2^2$$
$$\Theta_4 = 3u_4u_2 - 5u_3^2 \qquad \Theta_5 = 9u_5u_2^2 - 45u_4u_3u_2 + 40u_3^3$$
$$\Theta_6 = 9u_6u_2^3 - 63u_5u_3u_2^2 - 45u_4^2u_2^2 + 255u_4u_3^2u_2 - 160u_3^4$$
$$\begin{aligned}\Theta_8 = {} & (9/2)\left[18u_7u_2^4(\Theta_5) - 189u_6^2u_2^6 + 126u_6u_2^4(9u_5u_3u_2 + 15u_4^2u_2 - 25u_4u_3^2)\right.\\ & - 189u_5^2u_2^4(4u_3^2 + 15u_2u_4) + 210u_5u_3u_2^2(63u_4^2u_2^2 - 60u_4u_3^2u_2 + 32u_3^4)\\ & \left.-525u_4u_2(9u_4^3u_2^3 + 15u_4^2u_3^2u_2^2 - 60u_4u_3^4u_2 + 64u_3^6) + 11200u_3^8\right]\end{aligned}$$
$$\begin{aligned}\Theta_8 = {} & (243/2)(u_2^4)\left[2u_8u_2(\Theta_5)^2 - 8u_7(\Theta_5)(9u_6u_2^3 - 36u_5u_3u_2^2 - 45u_4^2u_2^2\right.\\ & + 120u_4u_3^2u_2 - 40u_3^4) + 504u_6^3u_2^5 - 504u_6^2u_2^3(9u_5u_3u_2 + 15u_4^2u_2 - 25u_4u_3^2)\\ & + 28u_6(432u_5^2u_3^2u_2^3 + 243u_5^2u_4u_2^4 - 1800u_5u_4u_3^3u_2^2 - 240u_5u_3^5u_2 + 540u_5u_4^2u_3u_2^3\\ & + 6600u_4^2u_3^4u_2 - 2000u_4u_3^6 - 5175u_4^3u_3^2u_2^2 + 1350u_4^4u_2^3) - 2835u_5^4u_2^4\\ & + 252u_5^3u_3u_2^2(9u_4u_2 - 136u_3^2) - 35840u_5^2u_3^6 - 630u_5^2u_4u_2(69u_4^2u_2^2 - 160u_3^4 - 153u_4u_3^2u_2)\\ & \left.+2100u_5u_4^2u_3(72u_3^4 + 63u_4^2u_2^2 - 193u_4u_3^2u_2) - 7875u_4^4(8u_4^2u_2^2 - 22u_4u_3^2u_2 + 9u_3^4)\right]\end{aligned}$$
$$\Theta_9 = u_4\Theta_1^2 - 5u_1u_2(u_3\Theta_1 + \Theta_3)$$

Table 4.1: Differential functions in $u_k = y^{(k)}$ used construct invariants

4.1.1 Invariants are Separating

In this section we will work towards showing that each pair of invariants in (4.3) is a classifying pair of invariants for the associated action. We use the $\mathcal{I}^{\mathcal{SE}} = \{K_1^{\mathcal{SE}}, K_2^{\mathcal{SE}}\}$ to refer to the pair of invariants in (4.3) for the prolonged action of $\mathcal{SE}(2)$, and similarly denote the pairs of invariants for the prolonged actions of the other groups.

Proposition 4.1.1. $K_1^{\mathcal{SE}}$ separates orbits on the Zariski open set $W^2 \subset J^2$ and the set $\mathcal{I}^{\mathcal{SE}}$ separates orbits on the Zariski open set $W^3 \subset J^3$, where

$$W^3 = \left\{ \left(x, y, y^{(1)}, y^{(2)}, y^{(3)} \right) \in J^3 \,|\, \Theta_1 \neq 0 \right\}$$

and $W^2 = \pi_2^3(W^3) \subset J^2$ for the prolonged action of $\mathcal{SE}(2)$ on $\mathbb{C}^2$.

Proof. Note that W^2, W^3 are invariant subsets of J^2, J^3 under the prolonged action of $\mathcal{SE}(2)$. Take the point $p^{(2)} \in W^2 \subset J^2$, $p^{(2)} = \left(x, y, y^{(1)}, y^{(2)}\right)$.

First we will show that $K_1^{\mathcal{SE}}$ separates orbits on W^2. Through a series of transformations well-defined for any $p^{(2)} \in W^2$, one can find a point on the same orbit of the form $\overline{p}^{(2)} = \left(0, 0, 0, \overline{y}_p^{(2)}\right)$ where $\overline{y}^{(2)} \in \mathbb{C}$. Thus for any two points $p^{(2)}$, $q^{(2)} \in W^2$ where $K_1^{\mathcal{SE}}(p^{(2)}) = K_1^{\mathcal{SE}}(q^{(2)})$, we can instead compare $K_1^{\mathcal{SE}}(\overline{p}^{(2)}) = K_1^{\mathcal{SE}}(\overline{q}^{(2)})$.

Since $p^{(2)} \in W^2$, the equation $\omega^2 = 1 + \left(y^{(1)}\right)^2$ has two solutions over $\mathbb{C}$; let $\tilde{\omega} \neq 0$ be one of those solutions. Then the transformation $g_p \in \mathcal{SE}(2)$ defined by

$$c = \frac{1}{\tilde{\omega}}, \quad s = \frac{y^{(1)}}{\tilde{\omega}}, \quad a = -(cx + sy), \quad b = -(-sx + cy), \tag{4.4}$$

brings the point $p^{(n)}$ to

$$\overline{p}^{(2)} = \left(0, 0, 0, \overline{y}_p^{(2)}\right)$$

where $\overline{y}_p^{(2)} \in \mathbb{C}$ is the value

$$\overline{y}_p^{(2)} = \ -y^{(2)}\tilde{\omega}.$$

Now suppose that $K_1^{\mathcal{SE}}(p^{(2)}) = K_1^{\mathcal{SE}}(q^{(2)})$ for some $q^{(2)} \in J^2$. Since $K_1^{\mathcal{SE}}$ is invariant under the action of $\mathcal{SE}(2)$,

$$K_1^{\mathcal{SE}}(\overline{p}) = K_1^{\mathcal{SE}}(p) = K_1^{\mathcal{SE}}(q) = K_1^{\mathcal{SE}}(\overline{q}^{(2)}),$$

for $\overline{q}^{(2)} = g_q \cdot q^{(2)}$ defined similarly as for $p^{(2)}$. This implies, from the formula of $K_1^{\mathcal{SE}}$ in terms of jet coordinates, that $\left(\overline{y}_p^{(2)}\right)^2 = \left(\overline{y}_q^{(2)}\right)^2$. Then either $\overline{y}_p^{(2)} = \overline{y}_q^{(2)}$ or $\overline{y}_p^{(2)} = -\overline{y}_q^{(2)}$.

In the case that $\overline{p}^{(2)} = \overline{q}^{(2)}$, $p^{(2)}$ and $q^{(2)}$ are clearly in the same orbit. Denote $g_{-1} \in \mathcal{SE}(2)$ to be the transformation

$$c = -1, \quad s = 0, \quad a = 0, \quad b = 0.$$

Then if $\overline{y}_p^{(2)} = -\overline{y}_q^{(2)}$,

$$g_{-1} \cdot \overline{p}^{(2)} = \overline{q}^{(2)}$$

and hence $p^{(2)}$ and $q^{(2)}$ lie in the same orbit. Thus $K_1^{\mathcal{SE}}$ separates orbits on $W^2 \subset J^2$. For $p^{(3)}, q^{(3)} \in W^3 \subset J^3$, $K_1^{\mathcal{SE}}(p^{(3)}) = K_1^{\mathcal{SE}}(q^{(3)})$, and $K_2^{\mathcal{SE}}(p^{(3)}) = K_2^{\mathcal{SE}}(q^{(3)})$, we have shown above that there exists a representative of each point's orbit such that

$$\overline{p}^{(3)} = \left(0, 0, 0, \overline{y}_p^{(2)}, \overline{y}_p^{(2)}\right), \quad \overline{q}^{(3)} = \left(0, 0, 0, \overline{y}_p^{(2)}, \overline{y}_q^{(3)}\right).$$

Thus, since $K_2^{\mathcal{SE}}$ is constant on each orbit, $K_2^{\mathcal{SE}}(\overline{p}^{(3)}) = K_2^{\mathcal{SE}}(\overline{q}^{(3)})$, which implies that $\overline{y}_p^{(3)} = \overline{y}_q^{(3)}$. Thus $p^{(3)}$ and $q^{(3)}$ must lie in the same orbit, showing that $\mathcal{I}^{\mathcal{SE}}$ separates orbits on W^3. □

Proposition 4.1.2. $K_1^{\mathcal{E}}$ separates orbits on the Zariski open set $W^2 \subset J^2$ and the set $\mathcal{I}^{\mathcal{E}}$ separates orbits on the Zariski open set $W^3 \subset J^3$, where

$$W^3 = \left\{ \left(x, y, y^{(1)}, y^{(2)}, y^{(3)}\right) \in J^3 \,|\, \Theta_1 \neq 0 \right\}$$

and $W^2 = \pi_2^3(W^3) \subset J^2$ for the action of $\mathcal{E}(2)$ on $\mathbb{C}^2$.

Proof. Note that W^2, W^3 are invariant subsets of J^2, J^3 under the prolonged action of $\mathcal{E}(2)$. Since $K_1^{\mathcal{SE}} = K_1^{\mathcal{E}}$ and $\mathcal{SE}(2)$ is a subgroup of $\mathcal{E}(2)$, the same argument in the proof of Proposition 4.1.1 shows that $K_1^{\mathcal{SE}}$ separates points on W^2. Thus for $p^{(3)}, q^{(3)} \in W^3 \subset J^3$, when $K_1^{\mathcal{E}}(p^{(3)}) = K_1^{\mathcal{E}}(q^{(3)})$, there exists a representative of each point's orbit such that

$$\overline{p}^{(3)} = \left(0, 0, 0, \overline{y}_p^{(2)}, \overline{y}_p^{(2)}\right), \quad \overline{q}^{(3)} = \left(0, 0, 0, \overline{y}_p^{(2)}, \overline{y}_q^{(3)}\right),$$

using the same transformation (4.4). Since $K_2^{\mathcal{E}}$ is constant on each orbit, $K_2^{\mathcal{E}}(\overline{p}^{(3)}) = K_2^{\mathcal{E}}(\overline{q}^{(3)})$, implies that $\left(\overline{y}_p^{(3)}\right)^2 = \left(\overline{y}_q^{(3)}\right)^2$.

Either $\overline{y}_p^{(3)} = \overline{y}_q^{(3)}$ or $\overline{y}_p^{(3)} = -\overline{y}_q^{(3)}$. In the case that $\overline{p}^{(3)} = \overline{q}^{(3)}$, $p^{(3)}$ and $q^{(3)}$ are clearly in the same orbit. The reflection g_R defined by the transformation

$$g_R = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

maps points $\left(x, y, y^{(1)]}, y^{(2)}, y^{(3)}\right)$ to $\left(-x, y, -y^{(1)}, y^{(2)}, -y^{(3)}\right)$. Then if $\overline{y}_p^{(3)} = -\overline{y}_q^{(3)}$,

$$g_R \cdot \overline{p}^{(3)} = \overline{q}^{(3)}$$

and hence $p^{(3)}$ and $q^{(3)}$ lie in the same orbit. Thus $\mathcal{I}^{\mathcal{E}}$ separates orbits on $W^3 \subset J^3$. □

Proposition 4.1.3. $K_1^{\mathcal{S}}$ separates orbits on the Zariski open set $W^3 \subset J^3$ and the set $\mathcal{I}^{\mathcal{S}}$ separates orbits on the Zariski open set $W^4 \subset J^4$, where

$$W^4 = \left\{ \left(x, y, y^{(1)}, y^{(2)}, y^{(3)}, y^{(4)} \right) \in J^4 \,|\, \Theta_1, \Theta_2 \neq 0 \right\}$$

and $W^3 = \pi_3^4(W^4) \subset J^3$ for the action of $\mathcal{S}(2)$ on $\mathbb{C}^2$.

Proof. Note that W^3, W^4 are invariant subsets of J^3, J^4 under the prolonged action of $\mathcal{S}(2)$. Let $p^{(4)} = \left(x, y, y^{(1)}, \ldots, y^{(3)}\right)$ be a point in $W^3 \subset J^3$. Then the transformation $g_p \in \mathcal{S}(2)$ defined by

$$a = \frac{-y^{(2)}\left(yy^{(1)} + x\right)}{\left(\left(y^{(1)}\right)^2 + 1\right)^2}, \qquad b = \frac{y^{(2)}\left(xy^{(1)} - y\right)}{\left(\left(y^{(1)}\right)^2 + 1\right)^2}$$
$$c = \frac{y^{(2)}}{\left(\left(y^{(1)}\right)^2 + 1\right)^2}, \qquad s = \frac{y^{(1)}y^{(2)}}{\left(\left(y^{(1)}\right)^2 + 1\right)^2},$$

brings the point $p^{(3)}$ to

$$\overline{p}^{(3)} = \left(0, 0, 0, 1, \overline{y}_p^{(3)}\right)$$

for some $\overline{y}_p^{(3)} \in \mathbb{C}$. Now suppose that $K_1^{\mathcal{S}}(p^{(3)}) = K_1^{\mathcal{S}}(q^{(3)})$ for some $q^{(3)} \in J^3$. Since $K_1^{\mathcal{S}}$ is a differential invariant

$$K_1^{\mathcal{S}}(\overline{p}^{(3)}) = K_1^{\mathcal{S}}(p^{(3)}) = K_1^{\mathcal{A}}(q^{(3)}) = K_1^{\mathcal{S}}(\overline{q}^{(3)}),$$

for $\overline{q}^{(3)} = g_q \cdot q^{(3)}$ defined similarly as for $p^{(3)}$. This implies from the formula of $K_1^{\mathcal{S}}$, that $\overline{y}_p^{(3)} = \overline{y}_q^{(3)}$, and hence $p^{(3)}$ and $q^{(3)}$ lie in the same orbit. Thus $K_1^{\mathcal{S}}$ separates orbits on W^3. For $p^{(4)}, q^{(4)} \in J45$, $K_1^{\mathcal{S}}(p^{(4)}) = K_1^{\mathcal{SA}}(q^{(4)})$, and $K_2^{\mathcal{S}}(p^{(4)}) = K_2^{\mathcal{S}}(q^{(4)})$, we have shown above that there exists a representative of each point's orbit such that

$$\overline{p}^{(4)} = \left(0, 0, 0, 1, \overline{y}_p^{(3)}, \overline{y}_p^{(4)}\right), \quad \overline{q}^{(4)} = \left(0, 0, 0, 1, \overline{y}_p^{(3)}, \overline{y}_q^{(4)}\right).$$

Since $K_2^{\mathcal{S}}$ is constant on each orbit, $K_2^{\mathcal{S}}(\overline{p}^{(4)}) = K_2^{\mathcal{S}}(\overline{q}^{(4)})$, which implies that $\overline{y}_p^{(4)} = \overline{y}_q^{(4)}$. Thus p and q must lie in the same orbit, showing that $\mathcal{I}^{\mathcal{S}}$ separates orbits on W^4. □

Proposition 4.1.4. $K_1^{\mathcal{SA}}$ separates orbits on the Zariski open set $W^4 \subset J^4$ and the set $\mathcal{I}^{\mathcal{SA}}$ separates orbits on the Zariski open set $W^5 \subset J^5$, where

$$W^5 = \left\{ p^{(5)} \in J^5 \,|\, y^{(2)} \neq 0 \right\},$$

and $W^4 = \pi_4^5(W^5) \subset J^4$, for the action of $\mathcal{SA}(2)$ on $\mathbb{C}^2$.

Proof. Note that W^4, W^5 are invariant subsets of J^4, J^5 under the prolonged action of $\mathcal{SA}(2)$. Let $p^{(4)} = \left(x, y, y^{(1)}, \ldots, y^{(4)}\right)$ be a point in $W^4 \subset J^4$. Note the equation $\omega^3 = y^{(2)}$ has three solutions over $\mathbb{C}$ when $p^{(4)} \in W^4$; let $\tilde{\omega} \neq 0$ be one of those solutions. Then the transformation $g_p \in \mathcal{SA}(2)$ defined by

$$a_1 = \frac{3\left(y^{(2)}\right)^2 - y^{(3)}y^{(1)}}{\tilde{\omega}^5}, \qquad a_2 = \frac{y^{(3)}}{3\tilde{\omega}^5}$$
$$a_3 = \frac{3y^{(3)}y^{(1)}x - 9\left(y^{(2)}\right)^2 x - y^{(3)}y}{\tilde{\omega}^5}, \qquad a_4 = \frac{-y^{(1)}}{\tilde{\omega}},$$
$$a_5 = \frac{1}{\tilde{\omega}}, \qquad a_6 = \frac{y^{(1)}x - y}{\tilde{\omega}}$$

brings the point $p^{(4)}$ to

$$\overline{p}^{(4)} = \left(0, 0, 0, 1, 0, \overline{y}_p^{(4)}\right)$$

for some $\overline{y}_p^{(4)} \in \mathbb{C}$. Now suppose that $K_1^{\mathcal{SA}}(p^{(4)}) = K_1^{\mathcal{SA}}(q^{(4)})$ for some $q^{(4)} \in J^4$. Since $K_1^{\mathcal{SA}}$ is a differential invariant

$$K_1^{\mathcal{SA}}(\overline{p}^{(4)}) = K_1^{\mathcal{SA}}(p^{(4)}) = K_1^{\mathcal{SA}}(q^{(4)}) = K_1^{\mathcal{SA}}(\overline{q}^{(4)}),$$

for $\overline{q}^{(4)} = g_q \cdot q^{(4)}$ defined similarly as for $p^{(4)}$. This implies from the formula of $K_1^{\mathcal{SA}}$, that $\overline{y}_p^{(4)} = \overline{y}_q^{(4)}$, and hence $p^{(4)}$ and $q^{(4)}$ lie in the same orbit. Thus $K_1^{\mathcal{SA}}$ separates orbits on W^4. For $p^{(5)}, q^{(5)} \in J^5$, $K_1^{\mathcal{SA}}(p^{(5)}) = K_1^{\mathcal{SA}}(q^{(5)})$, and $K_2^{\mathcal{SA}}(p^{(5)}) = K_2^{\mathcal{SA}}(q^{(5)})$, we have shown above that there exists a representative of each point's orbit such that

$$\overline{p}^{(5)} = \left(0, 0, 0, 1, 0, \overline{y}_p^{(4)}, \overline{y}_p^{(5)}\right), \quad \overline{q}^{(5)} = \left(0, 0, 0, 1, 0, \overline{y}_p^{(4)}, \overline{y}_q^{(5)}\right).$$

Since $K_2^{\mathcal{SA}}$ is constant on each orbit, $K_2^{\mathcal{SA}}(\overline{p}^{(5)}) = K_2^{\mathcal{SA}}(\overline{q}^{(5)})$, which implies that $\overline{y}_p^{(5)} = \overline{y}_q^{(5)}$. Thus p and q must lie in the same orbit, showing that $\mathcal{I}^{\mathcal{SA}}$ separates orbits on W^5. □

Proposition 4.1.5. $K_1^{\mathcal{A}}$ separates orbits on the Zariski open set $W^5 \subset J^5$ and the set $\mathcal{I}^{\mathcal{A}}$ separates orbits on the Zariski open set $W^6 \subset J^6$, where

$$W^6 = \left\{p^{(6)} \in J^6 \,|\, \Theta_2, \Theta_4 \neq 0\right\}$$

and $W^5 = \pi_5^6(W^6) \subset J^5$, for the action of $\mathcal{A}(2)$ on $\mathbb{C}^2$.

Proof. Note that W^5, W^6 are invariant subsets of J^5, J^6 under the prolonged action of $\mathcal{A}(2)$. Let $p^{(5)} = \left(x, y, y^{(1)}, \ldots, y^{(5)}\right)$ be a point in $W^5 \subset J^5$. Note the equation $\omega^2 = \Theta_4$ has two

solutions over $\mathbb{C}$ when $p^{(5)} \in W^5$; let $\tilde{\omega} \neq 0$ be one of those solutions. Then for $p \in W^5$, the transformation $g_p \in \mathcal{A}(2)$ defined by

$$a_1 = \frac{-\tilde{\omega}\left(y^{(1)}y^{(3)} - 3\left(y^{(2)}\right)^2\right)}{\left(9y^{(2)}\right)^3}, \qquad a_2 = \frac{\tilde{\omega}y^{(3)}}{\left(9y^{(2)}\right)^3}$$
$$a_3 = \frac{\tilde{\omega}\left(xy^{(1)}y^{(3)} - 3x\left(y^{(2)}\right)^2 - yy^{(3)}\right)}{\left(9y^{(2)}\right)^3}, \qquad a_4 = \frac{-\Theta_4 y^{(1)}}{\left(9y^{(2)}\right)^3},$$
$$a_5 = \frac{\Theta_4}{\left(9y^{(2)}\right)^3}, \qquad a_6 = \frac{\Theta_4\left(xy^{(1)} - y\right)}{\left(9y^{(2)}\right)^3}$$

brings the point $p^{(5)}$ to

$$\overline{p}^{(5)} = \left(0, 0, 0, 1, 0, 3, \overline{y}_p^{(5)}\right)$$

for some $\overline{y}_p^{(5)} \in \mathbb{C}$. Now suppose that $K_1^{\mathcal{A}}(p^{(5)}) = K_1^{\mathcal{A}}(q^{(5)})$ for some $q^{(5)} \in J^5$. Since $K_1^{\mathcal{A}}$ is a differential invariant

$$K_1^{\mathcal{A}}(\overline{p}^{(5)}) = K_1^{\mathcal{A}}(p^{(5)}) = K_1^{\mathcal{A}}(q^{(5)}) = K_1^{\mathcal{A}}(\overline{q}^{(5)}),$$

for $\overline{q}^{(5)} = g_q \cdot q^{(5)}$ defined similarly as for $p^{(5)}$. This implies from the formula of $K_1^{\mathcal{A}}$, that $\left(\overline{y}_p^{(5)}\right)^2 = \left(\overline{y}_q^{(5)}\right)^2$. Either $\overline{y}_p^{(5)} = \overline{y}_q^{(5)}$ or $\overline{y}_p^{(5)} = -\overline{y}_q^{(5)}$. In the case that $\overline{p}^{(5)} = \overline{q}^{(5)}$, $p^{(5)}$ and $q^{(5)}$ are clearly in the same orbit. Denote g_R to be the transformation

$$g_R = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

Then if $\overline{y}_p^{(5)} = -\overline{y}_q^{(5)}$,

$$g_R \cdot \overline{p}^{(5)} = \overline{q}^{(5)}$$

and hence $p^{(5)}$ and $q^{(5)}$ lie in the same orbit. Thus $K_1^{\mathcal{A}}$ separates orbits on W^5. For $p^{(5)}, q^{(5)} \in J^6$ and $K_1^{\mathcal{A}}(p^{(6)}) = K_1^{\mathcal{A}}(q^{(6)}), K_2^{\mathcal{A}}(p^{(6)}) = K_2^{\mathcal{A}}(q^{(6)})$, we have shown above that there exists a representative of each point's orbit such that

$$\overline{p}^{(6)} = \left(0, 0, 0, 1, 0, 3, \overline{y}_p^{(5)}, \overline{y}_p^{(6)}\right), \quad \overline{q}^{(6)} = \left(0, 0, 0, 1, 0, 3, \overline{y}_p^{(5)}, \overline{y}_q^{(6)}\right).$$

Thus, since $K_2^{\mathcal{A}}$ is constant on each orbit, $K_2^{\mathcal{A}}(\overline{p}^{(6)}) = K_2^{\mathcal{A}}(\overline{q}^{(6)})$, which implies that $\overline{y}_p^{(6)} = \overline{y}_q^{(6)}$.

Thus $p^{(6)}$ and $q^{(6)}$ must lie in the same orbit, showing that $\mathcal{I}^{\mathcal{A}}$ separates orbits on W^6. $\square$

Proposition 4.1.6. $K_1^{\mathcal{P}}$ separates orbits on the Zariski open set $W^7 \subset J^7$ and the set $\mathcal{I}^{\mathcal{P}}$ separates orbits on the Zariski open set $W^8 \subset J^8$, where

$$W^8 = \left\{ p^{(8)} \in J^8 \,|\, \Theta_1, \Theta_2, \Theta_5 \neq 0 \right\}$$

and $W^7 = \pi_7^8(W^8) \subset J^7$, for the action of $\mathcal{PGL}(3)$ on $\mathbb{C}^2$.

Proof. Note that W^7, W^8 are invariant subsets of J^7, J^8 under the prolonged action of $\mathcal{PGL}(3, \mathbb{C})$. Let $p^{(7)} = \left(x, y, y^{(1)}, \ldots, y^{(7)}\right) \in J^7$. Since $\mathcal{SE}(2)$ is a subgroup of $\mathcal{PGL}(3)$, using the transformation in (4.4) we can bring $p^{(7)}$ to the point

$$p_1^{(7)} = \left(0, 0, 0, y_1^{(2)}, \ldots, y_1^{(7)}\right).$$

Since $p_1^{(7)} \in W^7$, the equation $\xi^3 = y_1^{(2)}$ has three solutions over $\mathbb{C}$. Denote one of these as $\tilde{\xi} \neq 0$. Define the transformation $g_1 \in \mathcal{PGL}(3)$ by

$$g_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \tilde{\xi} & \frac{y_1^{(3)}}{3\tilde{\xi}^5} \\ 0 & 0 & \frac{1}{\tilde{\xi}} \end{bmatrix}.$$

This transformation is defined when $y_1^{(2)} \neq 0$. Since $y_1^{(2)} = 0$ if and only if $y^{(2)} = 0$, g_1 is well defined for all $p^{(7)} \in W^7$. Define $g_1 \cdot p_1^{(7)} = p_2^{(7)}$. Then

$$p_2^{(7)} = \left(0, 0, 0, 1, 0, y_2^{(4)}, \ldots, y_2^{(7)}\right).$$

Note that

$$y_2^{(5)} = \frac{\Theta_5}{9\left(y^{(2)}\right)^4 \left(\left(y^{(1)}\right)^2 + 1\right)^2},$$

and hence the equation $\zeta^3 = y_2^{(5)}$ has three solutions over $\mathbb{C}$. Let $\tilde{\zeta} \neq 0$ be one of those solutions, and define the transformation $g_2 \in \mathcal{PGL}(3)$ by

$$g_2 = \begin{bmatrix} 1 & i & j \\ 0 & h & ih \\ 0 & 0 & h^2 \end{bmatrix},$$

where

$$h = \tilde{\zeta},\ \ i = \frac{5\left(y_2^{(4)}\right)^2 - y_2^{(6)}}{3y_2^{(5)}},\ \ j = \frac{\left(y_2^{(6)}\right)^2 - 10y_2^{(6)}\left(y_2^{(4)}\right)^2 - 3\left(y_2^{(5)}\right)^2 y_2^{(4)} + 25\left(y_2^{(4)}\right)^4}{18\left(y_2^{(5)}\right)^2}.$$

Then $g_2 \cdot p_2^{(7)} = \overline{p}^{(7)}$ where

$$\overline{p}^{(7)} = \left(0, 0, 0, 1, 0, 0, 1, 0, \overline{y}_p^{(7)}\right).$$

Now suppose that $K_1^{\mathcal{P}}(p^{(7)}) = K_1^{\mathcal{P}}(q^{(7)})$ for any $p^{(7)}, q^{(7)} \in W^7 \subset J^7$. Since $K_1^{\mathcal{P}}$ is a differential invariant

$$K_1^{\mathcal{P}}(\overline{p}^{(7)}) = K_1^{\mathcal{P}}(p^{(7)}) = K_1^{\mathcal{P}}(q^{(7)}) = K_1^{\mathcal{P}}(\overline{q}^{(7)}),$$

for $\overline{q}^{(7)}$ defined similarly as $\overline{p}^{(7)}$. This implies from the formula of $K_1^{\mathcal{P}}$, that $\left(\overline{y}_p^{(7)}\right)^3 = \left(\overline{y}_q^{(7)}\right)^3$. Thus $\overline{y}_p^{(7)} = \omega \overline{y}_q^{(7)}$ where ω is a third root of unity. Let $g_\omega \in \mathcal{PGL}(3)$ be defined as

$$g_\omega = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \frac{1}{\omega} \end{bmatrix}.$$

Then $g_\omega \cdot \overline{p}^{(7)} = \overline{q}^{(7)}$. Therefore if $K_1^{\mathcal{P}}(p^{(7)}) = K_1^{\mathcal{P}}(q^{(7)})$, $p^{(7)}$ and $q^{(7)}$ lie in the same orbit of the prolongation of $\mathcal{PGL}(3)$. For $p^{(8)}, q^{(8)} \in W^8$ and $K_1^{\mathcal{P}}(p^{(8)}) = K_1^{\mathcal{P}}(q^{(8)}), K_2^{\mathcal{P}}(p^{(8)}) = K_2^{\mathcal{P}}(q^{(8)})$, we have shown above that there exists a representative of each point's orbit such that

$$\overline{p}^{(8)} = \left(0, 0, 0, 1, 0, 0, 1, 0, \overline{y}_p^{(7)}, \overline{y}_p^{(8)}\right), \quad \overline{q}^{(8)} = \left(0, 0, 0, 1, 0, 0, 1, 0, \overline{y}_p^{(7)}, \overline{y}_q^{(8)}\right).$$

Since $K_2^{\mathcal{P}}$ is constant on each orbit, $K_2^{\mathcal{P}}(\overline{p}^{(8)}) = K_2^{\mathcal{P}}(\overline{q}^{(8)})$, which implies that $\overline{y}_p^{(8)} = \overline{y}_q^{(8)}$. Thus $\overline{p}^{(8)} = \overline{q}^{(8)}$, meaning p and q must lie in the same orbit, showing that $\mathcal{I}^{\mathcal{P}}$ separates orbits on W^8. □

Theorem 4.1.7. The pairs of invariants in (4.3) are classifying invariants for the actions of $\mathcal{SE}(2), \mathcal{E}(2), \mathcal{S}(2), \mathcal{SA}(2), \mathcal{A}(2)$, and $\mathcal{PGL}(3)$ on $\mathbb{C}^2$.

Proof. One can see that the invariants are of appropriate orders for each of the groups. Propositions 4.1.1 - 4.1.6 prove the result. □

From the formulas in (4.3) and Definition 3.1.13, we can identify the conditions that characterize exceptional curves for each of the classifying pairs of invariants.

Proposition 4.1.8. The exceptional curves with respect to $\mathcal{I}^{\mathcal{P}}$, $\mathcal{I}^{\mathcal{A}}$, and $\mathcal{I}^{\mathcal{SA}}$ are lines and conics. The $\mathcal{I}^{\mathcal{S}}$-exceptional curves are lines and circles, while the $\mathcal{I}^{\mathcal{SE}}$- and $\mathcal{I}^{\mathcal{E}}$-exceptional curves are lines. In particular, if $X = V(F)$ is a curve exceptional with respect to the classifying invariants in (4.3) then F has degree at most two.

Proof. Propositions 2 and 3 from Section 4.3 in [10] show that $\mathcal{I}^{\mathcal{A}}$- and $\mathcal{I}^{\mathcal{P}}$-exceptional curves are lines and conics and an analogous argument shows that this is the case for $\mathcal{I}^{\mathcal{SA}}$-exceptional curves as well.

A curve $X = V(F)$ being $\mathcal{I}^{\mathcal{SE}}$- or $\mathcal{I}^{\mathcal{SE}}$-exceptional is equivalent to the curve satisfying either $F_y \equiv 0$, $\Theta_1 \equiv 0$, or $\Theta_2 \equiv 0$, all of which imply X must a line. Conversely $\Theta_2 \equiv 0$ for any line. A curve being $\mathcal{I}^{\mathcal{S}}$-exceptional is equivalent to either one of the previous conditions or $\Theta_3 \equiv 0$. The result follows from the fact that $\Theta_3 \equiv 0$ if and only if X is a line or a circle. □

4.2 Generic properties of signature polynomials

For each of the classifying sets of invariants given in (4.3), we derive formulas for the degree of the signature polynomial of a generic curve in terms of the curve's degree. To do so we examine each term in the degree formula (3.10) of Theorem 3.2.1.

4.2.1 Generic degree

We start by looking at the rational functions defining the invariants (4.3).

Lemma 4.2.1. For a generic polynomial $F \in \mathbb{C}[x, y]$ of degree $d \geq 3$, the restrictions of the differential functions Θ_i to the curve $V(F)$ are equal to rational functions of the form $T_i(x, y)/(F_y)^{d_i}$ with $\deg(T_i) \leq \tau_i$ where τ_i, d_i are given as follows:

i	1	2	3	4	5	6	7	8	9
τ_i	$2d-2$	$3d-4$	$6d-8$	$8d-12$	$12d-18$	$16d-24$	$32d-48$	$48d-72$	$9d-12$
d_i	2	3	6	8	12	16	32	48	9

Proof. Using the form of each derivative function restricted to $X = V(F)$ as in Remark 3.1.1, one can evaluate the formulas given for $\Theta_1, \ldots, \Theta_9$ given in Table 4.1.

For example, plugging in the rational expressions for $y^{(n)}|_X$ to the differential formula for Θ_4 gives $\Theta_4 = \left(3P_4P_2 - 5(P_3)^2\right)/F_y^{10}$. See B.1 for explicit computations. The numerator has degree $10d - 14$, but it is also divisible by F_y^2. This gives an expression $\Theta_4 = T_4(x, y)/(F_y)^8$ where T_i has degree less than or equal to $8d - 12$. The arguments for the other differential functions follow similarly. □

Explicit formulas for the polynomials T_i are quite long. A code to compute them can be found in Appendix B.1. Note that for each of the classifying invariants, the partial derivative function F_y cancels out and leaves each invariant as a rational function of the polynomials $T_1, \ldots, T_9$.

In the following lemma, we use homogenizations of $T_1, \ldots, T_9$ to write down projective extensions $\boldsymbol{\sigma}$ of the signature maps for each pair of invariants (4.3).

Lemma 4.2.2. Fix an irreducible polynomial $F \in \mathbb{C}[x, y]$ of degree $d \geq 3$ and let $X = V(F)$. For $G = \mathcal{SE}, \mathcal{E}, \mathcal{S}, \mathcal{SA}, \mathcal{A}, \mathcal{P}$, let σ_X^G denote the signature map given by the invariants $\mathcal{I}^G$ in (4.3). Then

$$\begin{aligned} \boldsymbol{\sigma}^{\mathcal{SE}} &= [\mathbf{T}_1{}^3 : x_0^2\mathbf{T}_2{}^2 : x_0^2\mathbf{T}_3], & \boldsymbol{\sigma}^{\mathcal{E}} &= [\mathbf{T}_1{}^6 : x_0^2\mathbf{T}_1{}^3\mathbf{T}_2{}^2 : x_0^4\mathbf{T}_3{}^2], \\ \boldsymbol{\sigma}^{\mathcal{S}} &= [\mathbf{T}_2{}^3 : \mathbf{T}_9 : \mathbf{T}_2\mathbf{T}_3], & \boldsymbol{\sigma}^{\mathcal{SA}} &= [\mathbf{T}_2{}^8 : x_0^4\mathbf{T}_4{}^3 : x_0^2\mathbf{T}_2{}^4\mathbf{T}_5], \\ \boldsymbol{\sigma}^{\mathcal{A}} &= [\mathbf{T}_4{}^3 : \mathbf{T}_5{}^2 : \mathbf{T}_4\mathbf{T}_6], \quad \text{and} & \boldsymbol{\sigma}^{\mathcal{P}} &= [\mathbf{T}_5{}^8 : \mathbf{T}_7{}^3 : \mathbf{T}_5{}^4\mathbf{T}_8] \end{aligned} \tag{4.5}$$

are projective extensions of the respective maps σ_X^G, where for each i, $\mathbf{T}_i$ equals the homogenization, $x_0^{\tau_i} T_i(\frac{x_1}{x_0}, \frac{x_2}{x_0}) \in \mathbb{C}[x_0, x_1, x_2]$, of the polynomial T_i from Lemma 4.2.1. Moreover,

$$\begin{aligned} \deg(\boldsymbol{\sigma}^{\mathcal{SE}}) &= 6d - 6, & \deg(\boldsymbol{\sigma}^{\mathcal{E}}) &= 12d - 12, \\ \deg(\boldsymbol{\sigma}^{\mathcal{S}}) &= 9d - 12, & \deg(\boldsymbol{\sigma}^{\mathcal{SA}}) &= 24d - 32, \\ \deg(\boldsymbol{\sigma}^{\mathcal{A}}) &= 24d - 36, \quad \text{and} & \deg(\boldsymbol{\sigma}^{\mathcal{P}}) &= 96d - 144. \end{aligned}$$

Proof. First, we note that by Lemma 4.2.1, the coordinates of $\boldsymbol{\sigma}^G$ are homogeneous of the stated degrees and that by Proposition 4.1.8, X is non-exceptional with respect to each of the classifying sets of invariants in (4.3). Moreover, with $G = \mathcal{A}$, for a point $p \in X$ we see that,

$$\sigma_X^{\mathcal{A}}(p) \;=\; \left(\frac{\Theta_5(p)^2}{\Theta_4(p)^3}, \frac{\Theta_6(p)}{\Theta_4(p)^2}\right) \;=\; \left(\frac{T_5(p)^2}{T_4(p)^3}, \frac{T_6(p)}{T_4(p)^2}\right) \;=\; \left(\frac{\boldsymbol{\sigma}_1^{\mathcal{A}}(1,p)}{\boldsymbol{\sigma}_0^{\mathcal{A}}(1,p)}, \frac{\boldsymbol{\sigma}_2^{\mathcal{A}}(1,p)}{\boldsymbol{\sigma}_0^{\mathcal{A}}(1,p)}\right).$$

Here the middle equality follows from the fact that the factors of F_y given by the degrees d_i in Lemma 4.2.1 all cancel out in the above expressions. If $\boldsymbol{\sigma}^{\mathcal{A}}(p)$ is not defined then $\Theta_4(p) = 0$, meaning p is not $\mathcal{I}$-regular. Thus $\boldsymbol{\sigma}^{\mathcal{A}}(p)$ is defined at all but finitely many points of X. Analogous arguments show that for the remaining groups, $\boldsymbol{\sigma}^G$ is a projective extension of σ_X^G. □

For a generic curve of fixed degree $d \geq 4$, Proposition 2.3.20 implies that $|\operatorname{Sym}(X, G)| = 1$ and from Lemma 4.2.2 we know the degree and form of a projective extension for the signature map for each of the groups considered.

The remaining term in (3.10) left to examine is the sum of multiplicities of the base locus points of our chosen projective extensions. We first show that, for each projective extension, all

base locus points belonging to a generic curve are at infinity.

Lemma 4.2.3. For a generic polynomial $F \in \mathbb{C}[x,y]_{\leq d}$, the base locii of the maps in (4.5) contain no points of the form $[1:p] \in \mathbb{CP}^2$ where $F(p) = 0$.

Proof. For any point $p \in \mathbb{C}^2$, consider the set

$$\mathcal{V}_p^{\mathcal{A}} \;=\; \left\{F \in \mathbb{C}[x,y]_{\leq d} \,:\, F(p) = 0 \text{ and } [1:p] \text{ belongs to the base locus of } \boldsymbol{\sigma}^{\mathcal{A}}\right\}.$$

We consider this condition on the cofficients a polynomial $F = \sum_{i+j\leq d} c_{ij}x^iy^j$. Note that a point $[1:p]$ belongs to the base locus of the map $\boldsymbol{\sigma}^{\mathcal{A}}$ if and only if $T_4(p) = T_5(p) = 0$. As discussed in Lemma 4.2.1, T_4 and T_5 are polynomials functions of the partial derivatives of F, meaning that we can consider $T_4(p)$ and $T_5(p)$ as polynomials in the coefficients c_{ij}. This lets us express $\mathcal{V}_p^{\mathcal{A}}$ as the variety of $F(p)$, $T_4(p)$, and $T_5(p)$.

For $p = (0,0)$, we can use computational algebra techniques to find the codimension of this set. The highest order partial derivative appearing in the expressions for T_4 and T_5 has order 5. Therefore $T_4(0,0)$ and $T_5(0,0)$ can be written as polynomials of c_{ij} where $i+j \leq 5$. One can check (see B.2) that these three polynomials in $\mathbb{Q}[c_{ij} : i+j \leq 5]$ impose algebraically independent conditions, meaning that $\mathcal{V}_{(0,0)}^{\mathcal{A}}$ has codimension 3 in $\mathbb{C}[x,y]_{\leq d}$.

Now we claim that for any point $p \in \mathbb{C}^2$, a polynomial F belongs to $\mathcal{V}_p^{\mathcal{A}}$ if and only if its image under translation $\overline{F}(x,y) = F(x+p_1, y+p_2)$ belongs to $\mathcal{V}_{(0,0)}^{\mathcal{A}}$. Note that the partial derivative functions of F are invariant under translation, meaning that for all i,j we have that $\frac{\partial^{i+j}\overline{F}}{\partial x^i y^j}(x,y) = \frac{\partial^{i+j}F}{\partial x^i y^j}(x+p_1, y+p_2)$. Let $\overline{T}_4, \overline{T_5}$ denote the polynomials obtained from Lemma 4.2.1 from $\overline{F}$. Since these are functions of the partial derivatives of $\overline{F}$, they are also invariant under translations meaning $\overline{T}_i(x,y) = T_i(x+p_1, y+p_2)$.

Then F belongs to $\mathcal{V}_p^{\mathcal{A}}$ if and only if $F(p) = \overline{F}(0,0) = 0$, $T_4(p) = \overline{T_4}(0,0) = 0$, and $T_5(p) = \overline{T_5}(0,0) = 0$, which occurs if and only if $\overline{F} \in \mathcal{V}_{(0,0)}^{\mathcal{A}}$. This shows that the set of polynomials not satisfying the condition in the statement of Lemma 4.2.3 can be written as

$$\mathcal{V}^{\mathcal{A}} \;=\; \bigcup_{p\in\mathbb{C}^2} \mathcal{V}_p^{\mathcal{A}} \;=\; \left\{F(x-p_1, y-p_2) : F \in \mathcal{V}_{(0,0)}^{\mathcal{A}}\right\}$$

Then the dimension of $\mathcal{V}^{\mathcal{A}}$ is at most $\dim(\mathcal{V}_{(0,0)}^{\mathcal{A}}) + 2$. Since $\mathcal{V}_{(0,0)}^{\mathcal{A}}$ has codimension 3 in the space of polynomials $\mathbb{C}[x,y]_{\leq d}$, this means that $\mathcal{V}^{\mathcal{A}}$ has codimension ≥ 1. This shows that the base locus of $\boldsymbol{\sigma}^{\mathcal{A}}$ contains no point $[1:p]$ where $F(p) = 0$.

A similar argument goes through for the other projective extensions. Here a point $[1:p] \in \mathbb{CP}^2$

belongs to the base locus if and only if

$$T_1(p) = T_2(p) = T_3(p) = 0, \quad T_1(p) = T_3(p) = 0, \quad T_2(p) = T_9(p) = 0,$$
$$T_2(p) = T_4(p) = 0, \quad \text{or} \quad T_5(p) = T_7(p) = 0$$

for $\boldsymbol{\sigma}^{\mathcal{SE}}$, $\boldsymbol{\sigma}^{\mathcal{E}}$, $\boldsymbol{\sigma}^{\mathcal{S}}$, $\boldsymbol{\sigma}^{\mathcal{SA}}$, and $\boldsymbol{\sigma}^{\mathcal{P}}$ respectively. The highest order partial derivative appearing in each expression is $y^{(7)}$. Therefore the evaluations of the polynomials T_i at $p = (0, 0)$ belong to $\mathbb{Q}[c_{ij} : i + j \leq 7]$.

To follow through an argument analogous to that for $\boldsymbol{\sigma}^{\mathcal{A}}$, it suffices to show that each pair of polynomials evaluated at $p = (0, 0)$ along with $c_{0,0}$ are algebraically independent (see B.2). In the Euclidean case it suffices to show that $T_1(p), T_2(p)$, and $c_{0,0}$ are algebraically independent. □

To precisely compute intersection multiplicities at the points at infinity, we will parameterize a neighborhood of each point $\mathbf{p} = [0 : p] \in V(\mathbf{F})$ using a Laurent series (see Definition 2.2.41). We can then compute the valuation of the series obtained by evaluating each Θ_i along this parameterization.

Lemma 4.2.4. Let $\mathbf{F} \in \mathbb{C}[x_0, x_1, x_2]_d$ be a generic homogeneous polynomial of degree d. The neighborhood of any point $\mathbf{p} = [0 : p_1 : p_2]$ in $V(\mathbf{F})$ can be parametrized by $t \mapsto [\alpha(t)]$ where

$$\alpha \;=\; \left(t, 1, \sum_{j=0}^{\infty} a_j t^j\right) \;\in\; \mathbb{C}[[t]]^3.$$

Moreover, for any homogeneous polynomial $\mathbf{G} \in \mathbb{C}[x_0, x_1, x_2]$, the intersection multiplicity of $\mathbf{F}$ and $\mathbf{G}$ at $\mathbf{p}$ is given by $\text{val}(\mathbf{G}(\alpha))$.

Proof. By genericity we can assume that $\mathbf{F} \in \mathbb{C}[x_0, x_1, x_2]_d$ has the property that $\mathbf{F}(0, 0, 1) \neq 0$ and the discriminant of the univariate polynomial $F(0, 1, x_2)$ is nonzero. Then any point $\mathbf{p} \in V(\mathbf{F}) \cap V(x_0)$ will have $p_1 \neq 0$, meaning that we can take $p_1 = 1$.

Consider the restriction $H = \mathbf{F}(v, 1, w) \in \mathbb{C}[v, w]$ and variety $V(H) \subset \mathbb{C}^2$, which contains the point $(0, p_2)$. Again by genericity, we can assume that $H_w(0, p_2) = \frac{\partial \mathbf{F}}{\partial x_2}(\mathbf{p})$ is non-zero. The Lemma then follows from Theorem 2.2.42. □

Lemma 4.2.5. For $d \geq 3$, the set of points $(a_0, \ldots, a_8)$ that can be extended to the coefficients a parametrization α for some $\mathbf{F} \in \mathbb{C}[x_0, x_1, x_2]_d$ in Lemma 4.2.4 is Zariski-dense in $\mathbb{C}^9$.

Proof. Note that $(a_0, \ldots, a_8)$ can be extended to the coefficients of a parametrization α for a polynomial $\mathbf{F} \in \mathbb{C}[x_0, x_1, x_2]_d$ if and only if $\mathbf{F}(0, 1, a_0) = 0$, the derivative of $\mathbf{F}$ with respect to x_2 at this point in non-zero, and $j_X^{(8)}(0, a_0)$ equals $(0, a_0, 1!a_1, \ldots, 8!a_8)$, where X is the plane

curve defined by $\mathbf{F}(x_0, 1, x_2) = 0$. If $\mathbf{F}$ is irreducible, then it is obtained from $\mathbf{F}(x_0, 1, x_2)$ by homogenization. The result then follows from Lemma 3.1.15, since $\binom{d+2}{2} - 2 \geq \binom{3+2}{2} - 2 = 8$. □

Lemma 4.2.6. Let $F \in \mathbb{C}[x, y]_{\leq d}$ be a generic polynomial with degree $d \geq 3$ and let $\alpha(t)$ denote the parametrization given by Lemma 4.2.4 for its homogenezation $\mathbf{F}$. For sufficiently small $t \in \mathbb{C}^*$, the Laurent series $\beta = t^{-1}(\alpha_1(t), \alpha_2(t)) = \left(t^{-1}, \sum_{j=0}^{\infty} a_j t^{j-1}\right)$ parametrizes the curve $V(F)$. The differential functions Θ_i along this parametrization satisfy:

i	1	2	3	4	5	6	7	8	9
$\mathrm{val}(\Theta_i(\beta))$	0	3	4	8	15	19	40	60	5

Proof. First let us calculate the image of β in the jet space. For $(x, y) = (t^{-1}, t^j)$ with $j \geq 1$, the derivative of y with respect to x equals $-jt^{j+1}$. Repeated applications of $\frac{\partial}{\partial x}$ then yields that $y^{(k)}(x)$ equals $(-1)^k \prod_{i=0}^{k-1}(i + j)t^{j+k}$. By linearity, for $(x, y) = \beta$ and $k \geq 2$,

$$y^{(k)}(x) \quad = \quad (-1)^k \cdot \sum_{j=2}^{\infty} a_j t^{j+k-1} \cdot \prod_{i=0}^{k-1}(i + j - 1).$$

We can then evaluate the differential functions $\Theta_1, \ldots, \Theta_9$ on truncations of these formulas, where a_j are indeterminates. (See B.3) For example, evaluating Θ_4 and Θ_5 give

$$\begin{aligned} \Theta_4(\beta) &= -36 \cdot a_2 \cdot t^8 + \text{higher order terms}, \quad \text{and} \\ \Theta_5(\beta) &= -4320 \cdot (2a_3^3 - 3a_2a_3a_4 + a_2^2a_5) \cdot t^{15} + \text{higher order terms}. \end{aligned}$$

In each case, the leading coefficients are polynomials of $a_0, \ldots, a_8$. Therefore, by Lemma 4.2.5 and the genericity of F, we may assume that these leading coefficients do not vanish. □

Lemma 4.2.7. For a generic homogeneous polynomial $\mathbf{F} \in \mathbb{C}[x_0, x_1, x_2]_d$ with $d \geq 3$ and a point $\mathbf{p} = [0 : p_1 : p_2]$ in $V(\mathbf{F})$, we have

$$\begin{gathered} \mathrm{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\sigma}^{\mathcal{SE}}) = 0, \quad \mathrm{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\sigma}^{\mathcal{E}}) = 0, \quad \mathrm{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\sigma}^{\mathcal{S}}) = 2, \\ \mathrm{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\sigma}^{\mathcal{SA}}) = 16, \quad \mathrm{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\sigma}^{\mathcal{A}}) = 12, \quad \text{and} \quad \mathrm{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\sigma}^{\mathcal{P}}) = 72, \end{gathered}$$

where for each G, are the maps $\boldsymbol{\sigma}^G$ are given by Lemma 4.2.2 for $F = \mathbf{F}(1, x, y)$.

Proof. Let $\alpha \in \mathbb{C}[[t]]^3$ be the local parametrization guaranteed by Lemma 4.2.4. For each index $i = 1, \ldots, 9$, let v_i denote the valuation of $\mathbf{T}_i(\alpha)$. By the same lemma and the formulas in

Lemma 4.2.2, the desired intersection multiplicities are

$$\begin{aligned}
&\operatorname{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\sigma}^{\mathcal{SE}}) = \min\{3v_1, 2+2v_2, 2+v_3\}, \quad \operatorname{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\sigma}^{\mathcal{E}}) = \min\{6v_1, 2+3v_1+2v_2, 4+2v_3\},\\
&\operatorname{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\sigma}^{\mathcal{S}}) = \min\{3v_2, v_9, v_2+v_3\}, \quad \operatorname{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\sigma}^{\mathcal{SA}}) = \min\{8v_2, 4+3v_4, 2+4v_2+v_5\},\\
&\operatorname{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\sigma}^{\mathcal{A}}) = \min\{3v_4, 2v_5, v_4+v_6\}, \text{ and } \operatorname{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\sigma}^{\mathcal{P}}) = \min\{8v_5, 3v_7, 4v_5+v_8\}.
\end{aligned}$$

Let $\beta \in \mathbb{C}((t))^2$ be the tuple of Laurent series given by Lemma 4.2.6. Since $\mathbf{T}_i$ is homogeneous of degree τ_i and $\alpha = t \cdot (1, \beta)$, we see that

$$\mathbf{T}_i(\alpha) = \mathbf{T}_i(t, t\beta) = t^{\tau_i}\mathbf{T}_i(1, \beta) = t^{\tau_i}T_i(\beta).$$

By genericity, the coefficient of x^{d-1} in F_y is nonzero, meaning that the valuation of $F_y(\beta)$ is $-(d-1)$. This and the formulas $T_i = \Theta_i \cdot (F_y)^{d_i}$ from Lemma 4.2.1 give that

$$\begin{aligned}
v_i = \operatorname{val}(\mathbf{T}_i(\alpha)) = \tau_i + \operatorname{val}(T_i(\beta)) &= \tau_i + \operatorname{val}(\Theta_i(\beta)) + d_i \operatorname{val}(F_y(\beta))\\
&= \tau_i + \operatorname{val}(\Theta_i(\beta)) - d_i(d-1).
\end{aligned}$$

Then combining the data from Lemmas 4.2.1 and 4.2.6 gives that

$$v_1 = 0, \quad v_2 = 2, \quad v_3 = 2, \quad v_4 = 4, \quad v_5 = 9, \quad v_6 = 11, \quad v_7 = 24, \quad v_8 = 36, \quad \text{and} \quad v_9 = 2.$$

Then the minimums above are achieved by $3v_1 = 0$, $6v_1 = 0$, $v_9 = 2$, $8v_2 = 16$, $3v_4 = 12$, and $8v_5 = 72$. □

Theorem 4.2.8. Fix an irreducible polynomial $F \in \mathbb{C}[x, y]_{\leq d}$ of degree $d \geq 4$ and let $X = V(F)$. Let S_X^G denote the signature polynomials defined by the invariants in (4.3) for the corresponding group G. Then, when the symmetry group of X is finite,

$$\begin{gathered}
\deg(S_X^{\mathcal{SE}}) \leq 6d^2 - 6d, \quad \deg(S_X^{\mathcal{E}}) \leq 12d^2 - 12d, \quad \deg(S_X^{\mathcal{S}}) \leq 9d^2 - 14d,\\
\deg(S_X^{\mathcal{SA}}), \deg(S_X^{\mathcal{A}}) \leq 24d^2 - 48d, \quad \text{and} \quad \deg(S_X^{\mathcal{P}}) \leq 96d^2 - 216d.
\end{gathered}$$

Furthermore these bounds are tight for generic $F \in \mathbb{C}[x, y]_{\leq d}$.

Proof. First we calculate the degree of the signature polynomial for generic $F \in \mathbb{C}[x, y]_{\leq d}$. By Proposition 4.1.8, the curve X is non-exceptional for each set of invariants and we can apply Theorem 3.2.1. By Proposition 2.3.20, since X is a general curve of degree ≥ 4, its symmetry group is trivial, meaning $n = 1$. Let $\mathbf{F} \in \mathbb{C}[x_0, x_1, x_2]$ denote the homogenization of F and

$\boldsymbol{X} = V(\mathbf{F}) \in \mathbb{CP}^2$. For each of the signature maps $\boldsymbol{\sigma}$, Theorem 3.2.1 states that

$$\deg(S_X) \;=\; \deg(\mathbf{F}) \cdot \deg(\boldsymbol{\sigma}) - \sum_{\mathbf{p} \in Bl(\boldsymbol{\sigma})} \mathrm{mult}_{\mathbf{p}}(\mathbf{F}, \boldsymbol{\sigma}).$$

By genericity, $V(\mathbf{F})$ contains exactly d points with $x_0 = 0$. The multiplicities of the signature map at each point is given by Lemma 4.2.7. By Lemma 4.2.3, these are the only points of $V(\mathbf{F})$ in the base locii of each of the projective extensions. All together, this gives

$$\begin{aligned}
\deg(S_X^{\mathcal{SE}}) &= d \cdot (6d-6) - d \cdot (0) \;=\; 6d^2 - 6d, \\
\deg(S_X^{\mathcal{E}}) &= d \cdot (12d-12) - d \cdot (0) \;=\; 12d^2 - 12d, \\
\deg(S_X^{\mathcal{S}}) &= d \cdot (9d-12) - d \cdot (2) \;=\; 9d^2 - 14d, \\
\deg(S_X^{\mathcal{SA}}) &= d \cdot (24d-32) - d \cdot (16) \;=\; 24d^2 - 48d, \\
\deg(S_X^{\mathcal{A}}) &= d \cdot (24d-36) - d \cdot (12) \;=\; 24d^2 - 48d, \text{ and} \\
\deg(S_X^{\mathcal{P}}) &= d \cdot (96d-144) - d \cdot (72) \;=\; 96d^2 - 216d.
\end{aligned}$$

By Theorem 3.2.8 these are upper bounds for the degree of any signature polynomial of a curve of degree d. □

We note that for all groups we consider, for generic curves, the degree of the signature curve has a quadratic dependence on the degree of the original curve. The symmetry group of a generic curve is trivial, but many interesting and important curves have non-trivial symmetry groups. In accordance with the degree formula (3.10), these curves have lower degree signature. In Section 4.3, for the Fermat curves family under the projective and affine action, the growth of the signature curve degree is completely suppressed by the increase in the symmetry group size.

Remark 4.2.9. For the case when $G = \mathcal{SE}(2)$, one can follow the proof of Lemma 4.2.3 to show that, for a generic curve, there are no affine points in $V(\boldsymbol{\sigma}_0^{\mathcal{SE}}, \boldsymbol{\sigma}_1^{\mathcal{SE}})$, $V(\boldsymbol{\sigma}_1^{\mathcal{SE}}, \boldsymbol{\sigma}_2^{\mathcal{SE}})$, or $V(\boldsymbol{\sigma}_0^{\mathcal{SE}}, \boldsymbol{\sigma}_2^{\mathcal{SE}})$. One can then use the method in Lemma 4.2.7 to determine $\mathrm{mult}_{\mathbf{p}}(\mathbf{F}, (\boldsymbol{\sigma}^i)^{\mathcal{SE}})$, $i = 0, 1, 2$, where $(\boldsymbol{\sigma}^0)^{\mathcal{SE}} = [\boldsymbol{\sigma}_1^{\mathcal{SE}}, \boldsymbol{\sigma}_2^{\mathcal{SE}}]$ and $(\boldsymbol{\sigma}^1)^{\mathcal{SE}}, (\boldsymbol{\sigma}^2)^{\mathcal{SE}}$ are defined similarly.

Thus, using a similar argument as in the proof of Theorem 4.2.8, one can compute the highest degree in each variable in terms of d for a generic curve of degree d. This already reduces the monomial support and is a first step towards computing the Newton polytope of the signature polynomial for a generic curve of fixed degree under $\mathcal{SE}(2)$.

4.3 Fermat curves

In this section, we investigate the signature polynomials for the Fermat family of curves using the classifying pairs of invariants in (4.3). The d-th degree *Fermat curve*, denoted in this section by X_d, is the zero set over $\mathbb{C}^2$ of the polynomial $F_d(x, y) = x^d + y^d + 1$, whose homogenization is $\mathbf{F}_d(x_0, x_1, x_2) = x_0^d + x_1^d + x_2^d$.

Theorem 4.2.8 gives an upper bound for $\deg(S_{X_d})$ in terms of d. However, for most of the actions considered in this thesis, $\deg(S_{X_d})$ is much lower than for a generic curve of degree d. The symmetry group of the Fermat curves is often non-trivial, which lowers $\deg(S_{X_d})$.

Theorem 4.3.1. The symmetry group of the d-th degree Fermat curve with respect to full projective, affine, special affine, similarity, Euclidean, and special Euclidean groups are:

- $\mathrm{Sym}(X_d, \mathcal{PGL}(3)) = S_3 \rtimes (\mathbb{Z}_d \times \mathbb{Z}_d)$ of cardinality $6d^2$,
- $\mathrm{Sym}(X_d, \mathcal{A}(2)) = S_2 \rtimes (\mathbb{Z}_d \times \mathbb{Z}_d)$ of cardinality $2d^2$,
- $\mathrm{Sym}(X_d, \mathcal{SA}(2)) = \mathrm{Sym}(X_d, \mathcal{S}(2)) = \begin{cases} \mathbb{Z}_d & \text{of cardinality } d, \text{ when } d \text{ is odd} \\ \mathbb{Z}_2 \times \mathbb{Z}_d & \text{of cardinality } 2d, \text{ when } d \text{ is even,} \end{cases}$
- $\mathrm{Sym}(X_d, \mathcal{E}(2)) = \begin{cases} \mathbb{Z}_2 & \text{of cardinality 2, when } d \text{ is odd} \\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 & \text{of cardinality 8, when } d \text{ is even,} \end{cases}$ and
- $\mathrm{Sym}(X_d, \mathcal{SE}(2)) = \begin{cases} \mathbb{Z}_1 & \text{of cardinality 1, when } d \text{ is odd} \\ \mathbb{Z}_2 \times \mathbb{Z}_2 & \text{of cardinality 4, when } d \text{ is even.} \end{cases}$

Here S_k is the permutation group over k-elements and $\mathbb{Z}_k$ is the cyclic groups of k-elements.

Proof. In [53] it has been shown that $\mathrm{Sym}(X_d, \mathcal{PGL}(3))$ consists of compositions of permutations of the homogeneous coordinates $[x_0 : x_1 : x_2]$ and transformations scaling the coordinates by d-th roots of unity, *i.e.* $[x_0 : x_1 : x_2] \to [x_0 : \omega_1 x_1 : \omega_2 x_2]$, where ω_1 and ω_2 are d-th roots of 1. This shows the first result. Since $\mathrm{Sym}(X_d, \mathcal{A}(2))$ is the subgroup of $\mathrm{Sym}(X_d, \mathcal{PGL}(3))$ that fixes the homogenous coordinate x_0, in the second result S_3 must be replaced with S_2. In the third case, restriction of $\mathrm{Sym}(X_d, \mathcal{A}(2))$ to $\mathrm{Sym}(X_d, \mathcal{SA}(2))$ adds the condition that $\omega_2 = \omega_1^{-1}$, and $\mathbb{Z}_d \times \mathbb{Z}_d$ is replaced with $\mathbb{Z}_d$.

In the case of the remaining groups, the size of the symmetry group depends on whether d is odd or even. The groups $\mathrm{Sym}(X_d, \mathcal{SA}(2))$ and $\mathrm{Sym}(X_d, \mathcal{S}(2))$ consist of transformations of the form $[x_0 : x_1 : x_2] \to [x_0 : \omega x_1 : \omega x_2]$ in the case d is odd, where ω is some d-th root of 1. When d is even we add the additional generator given by $[x_0 : x_1 : x_2] \to [x_0 : -x_2 : x_1]$.

In the case of the special Euclidean group for odd d there are no non-trivial symmetries, while for even d the symmetry group is generated by two independent elements, each of

order two, namely $[x_0 : x_1 : x_2] \to [x_0 : -x_2 : x_1]$ and $[x_0 : x_1 : x_2] \to [x_0 : -x_1 : -x_2]$. Finally, for the Euclidean group we add the generator of order two given by the reflection $[x_0 : x_1 : x_2] \to [x_0 : x_1 : x_2]$ in either case. □

For the projective and for the affine groups, the cardinality of the symmetry groups depend quadratically on d. At the same time Theorem 4.2.8 shows that the degrees of generic signature curves depend quadratically on d. In fact, these quadratic dependencies cancel, and the degrees of signatures of the Fermat curves for these actions are independent of d.

Proposition 4.3.2. There exist projective extensions of $\sigma^{\mathcal{P}}_{X_d}$ and $\sigma^{\mathcal{A}}_{X_d}$ of degrees $6d$ and $8d$ respectively with empty base locus when $d \geq 8$.

Proof. We start with the affine group. If we make the substitution $a = x^{d-6}$ and $b = y^{d-6}$ to obtain the polynomial $\overline{F}_d = x^6a+y^6b+1$, we can express the polynomials defining the map $\boldsymbol{\sigma}^{\mathcal{A}}_{X_d}$ as polynomials in x, y, a, b and d. In Section C.1 we compute polynomials $\overline{\boldsymbol{\sigma}}_0, \overline{\boldsymbol{\sigma}_1}, \overline{\boldsymbol{\sigma}_2} \in \mathbb{Q}[x, y, a, b, d]$ such that $\overline{\boldsymbol{\sigma}}_i$ evaluated at $a = x^{d-6}, b = y^{d-6}$ gives $\boldsymbol{\sigma}_i$ where $\boldsymbol{\sigma} = [\boldsymbol{\sigma}_0, \boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2]$ is a projective extension of $\boldsymbol{\sigma}^{\mathcal{A}}_{X_d}$.

From the formula of $\overline{\boldsymbol{\sigma}}_i$, we can see that each $\boldsymbol{\sigma}_i$ is homogeneous of degree $6d$. A point $[1 : p] \in Bl(\boldsymbol{\sigma})$ if and only if p lies in the ideal

$$\langle x^6a + y^6b + 1, \overline{\boldsymbol{\sigma}}_0, \overline{\boldsymbol{\sigma}_1}, \overline{\boldsymbol{\sigma}_2}\rangle.$$

Computing a Gröbner basis for this ideal yields the condition that $d^3(d-3)(d-2)^2 = 0$, and hence it is empty unless $d = 0, 2$ or 3. The point $[0 : p] \in Bl(\boldsymbol{\sigma})$ if and only if p lies in the ideal

$$\langle x^6a + y^6b, \overline{\boldsymbol{\sigma}}_0, \overline{\boldsymbol{\sigma}_1}, \overline{\boldsymbol{\sigma}_2}\rangle.$$

We arrive at the condition that $b^6y^{36}(1 + d)^2 = 0$ by again computing a Gröbner basis. This implies that $p_2 = 0$ for $[0 : p_1 : p_2] \in Bl(\boldsymbol{\sigma})$, but $[0 : 1 : 0] \notin V(F_d)$. Thus $Bl(\boldsymbol{\sigma}) = \emptyset$. The argument for $\sigma^{\mathcal{P}}_{X_d}$ follows similarly, with supporting computations found in Section C.2. □

Theorem 4.3.3. The signature of the Fermat curve $V(x^d + y^d + 1) \subset \mathbb{C}^2$ has

- degree four for all $d \geq 3$ for the $\mathcal{PGL}(3)$-action.
- degree two for $d = 3$ and degree three for all $d \geq 4$ for the $\mathcal{A}(2)$-action.

Proof. For $d \leq 8$ the signature polynomais for X_d are computing directly in Section C.1 and C.2. Denote the signature polynomials for X_d as $S^{\mathcal{A}}_{X_d}$, $S^{\mathcal{P}}_{X_d}$ for the affine and projective groups respectively. By Proposition 4.3.2 and the degree formula in (3.10),

- $\deg(S^{\mathcal{A}}_{X_d}) = \frac{d(6d)}{2d^2} = 3$,

- $\deg(S^{\mathcal{P}}_{X_d}) = \frac{d(24d)}{6d^2} = 4$.

□

We present here the explicit formulas for signatures polynomials and observe that their coefficients (but not their degrees) depend on d. For the projective group the signature polynomial of the Fermat curve of degree $d > 2$ is:

$$\begin{aligned}
S^{\mathcal{P}}_{X_d}(\kappa_1,\kappa_2) \;=\; & 49392(d-2)^4d^3(d+1)^4(2d-1)^4\kappa_2^4 + 602112(d-2)^4d^3(d+1)^4(2d-1)^4\kappa_1\kappa_2^2 \\
& + 10584(d-2)^3d^2(d+1)^3(2d-1)^3\left(10d^2-3d+3\right)\left(34d^2-27d+27\right)\kappa_2^3 \\
& + 1835008(d-2)^4d^3(d+1)^4(2d-1)^4\kappa_1^2 - 9289728(d-2)^3d^2(d+1)^3(2d-1)^3\left(d^2-d+1\right)^2\kappa_1\kappa_2 \\
& + 61236(d-2)^2d(d+1)^2(2d-1)^2\left(d^2-d+1\right)\left(10d^2-3d+3\right)^2\left(16d^2-9d+9\right)\kappa_2^2 \\
& - 23328(d-2)^2d(d+1)^2(2d-1)^2\left(11792d^8-17376d^7+28152d^6-24424d^5+19473d^4-8940d^3\right. \\
& \left.+3358d^2-324d+81\right)\kappa_1 + 118098(d-2)(d+1)(2d-1)\left(d^2-d+1\right)^2\left(10d^2-3d+3\right)^4\kappa_2 \\
& + 531441d\left(d^2-d+1\right)^3\left(10d^2-3d+3\right)^4.
\end{aligned}$$

The signature polynomial of the Fermat curve of degree $d > 2$ under the affine action is:

$$\begin{aligned}
S^{\mathcal{A}}_{X_d}(\kappa_1,\kappa_2) \;=\; & (d-3)^2(d-2)d^2(d+1)(2d-1)^3\kappa_2^3 - (d-5)^3d(2d-1)^2\kappa_1^2 \\
& + 3(d-5)(d-2)d(d+1)(2d-1)^2(5d-11)\kappa_1\kappa_2 + 6(d-2)^2d(d+1)^2(2d-1)^2\left(d^2-4d+6\right)\kappa_2^2 \\
& + 2(d-2)^2(d+1)^2(2d-1)\left(15d^2-10d+18\right)\kappa_1 + 12(d-2)^3(d+1)^3(2d-1)\left(d^2-2d+3\right)\kappa_2 \\
& + 8(d-2)^4d(d+1)^4.
\end{aligned}$$

For $d = 3$, the coefficient of κ_2^3 vanishes and the degree of the signature polynomial drops to two. These expressions raise the interesting question of the significance of $S^{\mathcal{A}}_{X_d}$ and $S^{\mathcal{P}}_{X_d}$, when d is a non-integer rational number greater.

CHAPTER 5

Further Directions

In this chapter we detail some of the interesting questions and future avenues for exploration that arose as a consequence of the work in this thesis.

5.1 Numerical methods

The field of numerical algebraic geometry is concerned with numerically computing quantities associated with algebraic varieties, such as their degree or dimension. See [31] for a brief introduction or [3] for a more comprehensive description of numerical algebraic methods and how they are implemented in the software, Bertini [2]. As the main results of this thesis involve the degree of a signature curve, an algebraic variety, the question naturally arises of how these methods can be used to understand and compute signature polynomials.

Question. How can one use existing numerical methods to aide in computing the degree of the signature polynomial, other quantities related to an algebraic curve's signature, or the signature polynomial?

The algorithm described in Appendix A still relies largely on Gröbner basis computations. Many of the steps involve computing the degree of zero-dimensional ideals. *Can these steps be done numerically to decrease the time required to compute the degree bounds?* In [15] the authors propose an algorithm to numerically determine the degree of the image of a rational map, which was implemented in the Macaulay2 package, Numerical Implicization [14]. A comparison of methods for use in predicting the degree of signature polynomials would be interesting.

Prior knowledge of the degree of the signature curve can also aide in constructing a *witness set* for the signature curve, or a set of points corresponding to the intersection of a general linear space with the signature curve. This representation of a variety allows one to numerically perform various computations such as component sampling or membership testing. *Can one use witness sets to decide whether two algebraic curves have the same signature?*

5.2 Choice of classifying invariants

In Chapter 4 we fixed a classifying pair of invariants built from classical differential invariants. The form of the invariants heavily influenced the computation of the degree of a signature polynomial of a generic curve. Proposition 3.1.12 gives a description of the possible choices of classifying invariants based on an initial pair.

Question. What is the relationship between the choice of classifying invariants and the generic degree of the signature polynomial?

In particular how can one find the "best" choice of invariants, i.e. a pair of invariants giving the lowest possible generic degree? Given a classifying pair of invariants $\{K_1, K_2\}$, one can also choose $\{K_1, K_1^n K_2\}$ as a classifying pair for $n \in \mathbb{Z}_+$. Thus an upper bound on the generic degree seems unlikely for most groups.

While we show the existence of a classifying pair of invariants in Theorem 3.1.11, as detailed in Section 3.2.3, an interesting question would be to investigate the existence of a *real* classifying pair of invariants. As shown in [10] this would give a notion of a signature curve classifying the real points of algebraic curves under the real elements of subgroups of $\mathcal{PGL}(3)$.

5.3 Applications to Invariant Theory

There is a long connection between differential invariants and classical invariant theory. Application of differential invariants to the problems in classical invariant theory was first proposed by Sophus Lie [43]. The differential signature construction, in particular, has also been previously been used to study such problems. Differential signature constructions for homogeneous polynomials in two variables (binary forms) under linear changes of coordinates were first introduced by Olver [46] and applied to their symmetry groups computation in [4]. For polynomials in three variables (ternary forms) under linear changes of coordinates, sets of differential invariants that characterize equivalence classes were computed and explored in [39] and [26]. An algorithm using differential invariants is given in [41] to efficiently compute the canonical form and symmetry group of an arbitrary ternary cubic. In his thesis, Wears [55] considered differential signatures of polynomials in an arbitrary number of variables.

As shown in the proof of Theorem 3.2.7, for a polynomial $F(x, y, \mathbf{a}) = \sum_{i,j} a_{ij} x^i y^j$, of fixed degree d there exists a polynomial $P(\kappa_1, \kappa_2, \mathbf{a})$ such that $P|_{\mathbf{a}=\tilde{\mathbf{a}}} = S_{X_{\tilde{\mathbf{a}}}}$ for the curve $X_{\tilde{\mathbf{a}}} = V(F|_{\mathbf{a}=\tilde{\mathbf{a}}})$. We can write $P = \sum_{i,j} b_{ij} \kappa_1^i \kappa_2^j$ where $1 \leq i, j \leq D = deg_{\kappa_1,\kappa_2}(P)$ and $b_{ij} \in \mathbb{C}[\mathbf{a}]$. Since two curves are G-equivalent if and only if they have the same signature, the set $\{b_{ij}\}$ is a separating set of polynomial invariants for polynomials of degree d under G.

Question. Understand the relationship between the separating set of polynomial invariants $\{b_{ij}\}$ and the signature polynomial.

This gives an alternate method to compute a separating set of polynomial invariants for ternary forms under the action of a subgroup of $\mathcal{PGL}(3)$. In practice, however, computing the image of the signature map on $F(x, y, \mathbf{a})$ would be computationally expensive. For a generic conic under the action of $\mathcal{SE}(2)$ this computation was feasible. The signature polynomial for a generic conic is given by

$$
\begin{aligned}
S_X =& 2916 \left(4\,a_{00}a_{01}a_{20} - a_{00}{a_{11}}^2 - {a_{01}}^2 a_{20} + a_{01}a_{10}a_{11} - a_{01}{a_{10}}^2\right)^2 \kappa_1^6 \\
&+ 2916 \left(a_{01} + a_{20}\right)\left(4\,{a_{01}}^2 - 4\,a_{01}a_{20} + 3\,{a_{11}}^2 + 4\,{a_{20}}^2\right) \\
&\left(4\,a_{00}a_{01}a_{20} - a_{00}{a_{11}}^2 - {a_{0,1}}^2 a_{20} + a_{01}a_{10}a_{11} - a_{01}{a_{10}}^2\right)\kappa_1^5 \\
&+ 972 \left(4\,a_{00}a_{01}a_{20} - a_{00}{a_{11}}^2 - {a_{01}}^2 a_{20} + a_{01}a_{10}a_{11} - a_{01}{a_{10}}^2\right)^2 \kappa_1^4\kappa_2^2 + 729 \left(4\,a_{01}a_{20} - {a_{11}}^2\right)^3 \kappa_1^4 \\
&- 972 \left(a_{01} + a_{20}\right)\left(4\,a_{01}a_{20} - {a_{11}}^2\right)\left(4\,a_{00}a_{01}a_{20} - a_{0,0}{a_{11}}^2 - {a_{01}}^2 a_{20} + a_{01}a_{10}a_{11} - a_{01}{a_{10}}^2\right)\kappa_1^3\kappa_2^2 \\
&+ 108 \left(4\,a_{00}a_{01}a_{20} - a_{00}{a_{11}}^2 - {a_{01}}^2 a_{20} + a_{01}a_{10}a_{11} - a_{01}{a_{10}}^2\right)^2 \kappa_1^2\kappa_2^4 \\
&+ 4 \left(4\,a_{00}a_{01}a_{20} - a_{00}{a_{11}}^2 - {a_{01}}^2 a_{20} + a_{01}a_{10}a_{11} - a_{01}{a_{10}}^2\right)^2 \kappa_2^6
\end{aligned}
$$

Compare this to the separating set invariants for real conics described in Example 2.1.15. Again we see $\det(A), \det(B)$, and $\mathrm{tr}(B)$, but also an additional invariant $4a_{20}^2 - 2a_{02}a_{20} + 3a_{11}^2 + 4a_{20}^2$. These four invariants completely determine the signature polynomial and thus are a separating set of polynomial invariants.

Unfortunately we also see much redundant information in the signature polynomial. In particular the invariant $\det(A)$ appears in the coefficients multiple times, and is sometimes squared. *Can we use some subset of the monomial support of the signature polynomial to classify curves?*

We can also think of computing the signature polynomial of a degree d curve X as evaluating this separating set of invariants on X without knowing explicitly what they are. If we can determine the degree of each b_{ij} (through computation over a finite field, perhaps), then by computing enough signature polynomials, we can interpolate each b_{ij}. This gives yet another way to compute a separating set of polynomial invariants.

5.4 Other generic properties

Theorem 3.2.7 shows the existence of a particular monomial support of the signature polynomial for a generic curve of fixed degree. In Chapter 4 we found the degree of the signature polynomial for a general curve. A natural next step would be determine the Newton polytope of the signature polynomial for a generic curve. More generally one can ask:

Question. What algebraic curves can appear as a signature polynomial of an algebraic curve?

For a fixed curve X, different classifying pairs of invariants give rise to possible different signature curves. Proposition 3.1.12 gives a relationship between classifying invariants, and hence between different signature curves for the same X.

Both determining generic properties and the space of possible signature curves could potentially be useful in computing signature polynomial without Gröbner basis algorithms. For instance, prior knowledge of the monomial support would aide in interpolating signature polynomials.

REFERENCES

[1] Reza Aghayan, Tim Ellis, and Jamshid Dehmeshki. Planar numerical signature theory applied to object recognition. *J. Math. Imaging Vision*, 48(3):583–605, 2014.

[2] Daniel J. Bates, Jonathan D. Hauenstein, Andrew J. Sommese, and Charles W. Wampler. Bertini: Software for numerical algebraic geometry. Available at bertini.nd.edu with permanent doi: dx.doi.org/10.7274/R0H41PB5.

[3] Daniel J. Bates, Jonathan D. Hauenstein, Andrew J. Sommese, and Charles W. Wampler. *Numerically solving polynomial systems with Bertini*, volume 25 of *Software, Environments, and Tools*. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 2013.

[4] Irina A. Berchenko (Kogan) and Peter J. Olver. Symmetries of polynomials. *Journal of Symbolic Computations*, 29:485–514, 2000.

[5] L. Bernardin, P. Chin, P. DeMarco, K. O. Geddes, D. E. G. Hare, K. M. Heal, G. Labahn, J. P. May, J. McCarron, M. B. Monagan, D. Ohashi, and S. M. Vorkoetter. *Maple Programming Guide*. Maplesoft, 2015.

[6] Wilhelm Blaschke. *Vorlesungen über Differentialgeometrie und geometrische Grundlagen von Einsteins Relativitätstheorie. Band II. Affine Differentialgeometrie*. J. Springer, Springer, Bertin, 1923.

[7] Mireille Boutin. Numerically invariant signature curves. *Int. J. Computer vision*, 40:235–248, 2000.

[8] Daniel A. Brake, Daniel J. Bates, Wenrui Hao, Jonathan D. Hauenstein, Andrew J. Sommese, and Charles W. Wampler. Algorithm 976: `{B}ertini_real`: numerical decomposition of real algebraic curves and surfaces. *ACM Trans. Math. Software*, 44(1):Art. 10, 30, 2017.

[9] Bruno Buchberger. An algorithm for finding the basis elements of the residue class ring of a zero dimensional polynomial ideal. *J. Symbolic Comput.*, 41(3-4):475–511, 2006. Translated from the 1965 German original by Michael P. Abramson.

[10] Joseph M. Burdis, Irina A. Kogan, and Hoon Hong. Object-image correspondence for algebraic curves under projections. *SIGMA Symmetry Integrability Geom. Methods Appl.*, 9:Paper 023, 31, 2013.

[11] Eugenio Calabi, Peter J. Olver, Chehrzad Shakiban, Allen Tannenbaum, and Steven Haker. Differential and numerically invariant signatures curves applied to object recognition. *Int. J. Computer vision*, 26:Paper 107,135, 1998.

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

[13] Élie. Cartan. *Les problèmes d'équivalence*. Oeuvres completes, II, pp. 1311-1334. Gauthier-Villars, Paris, 1953.

[14] Justin Chen and Joe Kileel. NumericalImplicitization: A *Macaulay2* package. Version 1.0.4. Available at `https://github.com/Macaulay2/M2/tree/master/M2/Macaulay2/packages`.

[15] Justin Chen and Joe Kileel. Numerical implicitization for macaulay2, 2016.

[16] David Cox, John Little, and Donal O'Shea. *Using algebraic geometry*, volume 185 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1998.

[17] David A. Cox, John Little, and Donal O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer, Cham, fourth edition, 2015. An introduction to computational algebraic geometry and commutative algebra.

[18] David S. Dummit and Richard M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.

[19] Olivier Faugeras. Cartan's moving frame method and its application to the geometry and evolution of curves in the Euclidean, affine and projective planes. *Application of Invariance in Computer Vision, J.L Mundy, A. Zisserman, D. Forsyth (eds.) Springer-Verlag Lecture Notes in Computer Science*, 825:11–46, 1994.

[20] Jean-Charles Faugre. FGb: A Library for Computing Grbner Bases. In Komei Fukuda, Joris Hoeven, Michael Joswig, and Nobuki Takayama, editors, *Mathematical Software - ICMS 2010*, volume 6327 of *Lecture Notes in Computer Science*, pages 84–87, Berlin, Heidelberg, September 2010. Springer Berlin / Heidelberg.

[21] Mark Fels and Peter J. Olver. Moving Coframes. II. Regularization and Theoretical Foundations. *Acta Appl. Math.*, 55:127–208, 1999.

[22] Gerd Fischer. *Plane algebraic curves*, volume 15 of *Student Mathematical Library*. American Mathematical Society, Providence, RI, 2001. Translated from the 1994 German original by Leslie Kay.

[23] William Fulton. *Algebraic curves*. Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989. An introduction to algebraic geometry, Notes written with the collaboration of Richard Weiss, Reprint of 1969 original.

[24] Anna Grim and Chehrzad Shakiban. Applications of signature curves to characterize melanomas and moles. In *Applications of computer algebra*, volume 198 of *Springer Proc. Math. Stat.*, pages 171–189. Springer, Cham, 2017.

[25] Heinrich W. Guggenheimer. *Differential geometry*. McGraw-Hill Book Co., Inc., New York-San Francisco-Toronto-London, 1963.

[26] Gülden Gün Polat and Peter J. Olver. Joint differential invariants of binary and ternary forms. *preprint*, 2017. `http://www-users.math.umn.edu/~olver/a_/ternary.pdf`.

[27] Grigoriĭ Gurevich. *Foundations of the theory of algebraic invariants*. Noordhoff, 1964.

[28] Joe Harris. *Algebraic geometry*, volume 133 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. A first course, Corrected reprint of the 1992 original.

[29] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

[30] Brendan Hassett. *Introduction to algebraic geometry*. Cambridge University Press, Cambridge, 2007.

[31] Jonathan D. Hauenstein and Andrew J. Sommese. What is numerical algebraic geometry? [Foreword]. *J. Symbolic Comput.*, 79(part 3):499–507, 2017.

[32] Mark S. Hickman. Euclidean signature curves. *J. Math. Imaging Vision*, 43(3):206–213, 2012.

[33] Daniel J. Hoff and Peter J. Olver. Extensions of invariant signatures for object recognition. *J. Math. Imaging Vision*, 45(2):176–185, 2013.

[34] Daniel J. Hoff and Peter J. Olver. Automatic solution of jigsaw puzzles. *J. Math. Imaging Vision*, 49(1):234–250, 2014.

[35] Evelyne Hubert and Irina A. Kogan. Smooth and algebraic invariants of a group action: local and global construction. *Foundation of Computational Math. J.*, 7:4:345–383, 2007.

[36] Thomas W. Hungerford. *Algebra*, volume 73 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1980. Reprint of the 1974 original.

[37] Edward L. Ince. *Ordinary Differential Equations*. Dover Publications, New York, 1944.

[38] Irina Kogan, Michael Ruddy, and Cynthia Vinzant. Differential Signatures of Algebraic Curves. *arXiv:1812.11388*, 2018.

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

[40] Irina A. Kogan. Two algorithms for a moving frame construction. *Canad. J. Math.*, 55:266–291, 2003.

[41] Irina A. Kogan and Marc Moreno Maza. Computation of canonical forms for ternary cubics. *Proceedings of ISSAC ACM Press*, pages 151–160, 2002.

[42] John M. Lee. *Introduction to smooth manifolds*, volume 218 of *Graduate Texts in Mathematics*. Springer, New York, second edition, 2013.

[43] Sophus Lie. *Vorlesungen über continuierliche Gruppen mit Geometrischen und anderen Anwendungen*. Chelsea Publishing Co., Bronx, N.Y., 1971. Bearbeitet und herausgegeben von Georg Scheffers, Nachdruck der Auflage des Jahres 1893.

[44] Emilio Musso and Lorenzo Nicolodi. Invariant signatures of closed planar curves. *J. Math. Imaging Vision*, 35(1):68–85, 2009.

[45] Peter J. Olver. *Equivalence, invariants and Symmetry*. Cambridge University Press, 1995.

[46] Peter J. Olver. *Classical invariant theory*, volume 44 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1999.

[47] Peter J. Olver. Moving frames and singularities of prolonged group actions. *Selecta Math. (N.S.)*, 6(1):41–77, 2000.

[48] Peter J. Olver. Moving frames: a brief survey. In *Symmetry and perturbation theory (Cala Gonone, 2001)*, pages 143–150. World Sci. Publ., River Edge, NJ, 2001.

[49] Lev V. Ovsiannikov. *Group analysis of differential equations*. Academic Press Inc. [Harcourt Brace Jovanovich Publishers], New York, 1982. Translated from the Russian by Y. Chapovsky, Translation edited by William F. Ames.

[50] Igor R. Shafarevich. *Basic algebraic geometry. 1*. Springer, Heidelberg, third edition, 2013. Varieties in projective space.

[51] V. V. Shokurov. Riemann surfaces and algebraic curves. In *Algebraic geometry, I*, volume 23 of *Encyclopaedia Math. Sci.*, pages 1–166. Springer, Berlin, 1994.

[52] Tonny A. Springer. Linear algebraic groups. In *Algebraic geometry. IV*, pages 1–121. 1994.

[53] Pavlos Tzermias. The group of automorphisms of the Fermat curve. *J. Number Theory*, 53(1):173–178, 1995.

[54] È rnest B. Vinberg and Vladimir L. Popov. Invariant theory. In *Algebraic geometry, 4 (Russian)*, Itogi Nauki i Tekhniki, pages 137–314, 315. Akad. Nauk SSSR, Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow, 1989.

[55] Thomas Wears. *Signature Varieties of Polynomial Functions.* PhD thesis, North Carolina State University, 2011.

APPENDICES

APPENDIX A

Algorithms for Signature Polynomials

In this appendix we provide procedures in Maple 2017 [[5] for the computing signature polynomials for a given algebraic curve as well as computing the bounds of the signature's degree in (3.12) and (3.14). We only include the explicit code for signature polynomials of curves under the special Euclidean group using the classifying set of invariants in (4.3). For the remaining groups, the code is easily adaptable by modifying the procedure defining the invariants.

The following procedures rely on a variety of packages: *PolynomialIdeals*, *algcurves*, *Groebner*, *Physics*, *DifferentialGeometry*, *JetCalculus*, *ArrayTools*, *LinearAlgebra*. It is also necessary to setup a frame using the **DGSetup** command. For this reason, before running any of the procedures outlined below execute the following:

```
> with(PolynomialIdeals,algcurves,Groebner,Physics,DifferentialGeometry):
> with(JetCalculus,ArrayTools,LinearAlgebra):
> Preferences("JetNotation", "JetNotation2"): DGsetup([x], [y], M, 8, verbose):
```

A.1 Computing the Signature Polynomial

The restriction rational classifying invariants to an algebraic curve is a rational map. The signature polynomial can then be computed by finding a Gröbner basis for an elimination ideal. In practice, these methods are computationally intensive and rarely complete within a day in Maple 2017 for curves of degree four or higher under any of the actions considered in this thesis. Curves with large symmetry groups seem to be an exception; the size of the symmetry reduces the degree of the signature polynomial as one can see from (3.10). One can improve this by

using the *FGb* package which implements the Faugère F5 algorthim for computing Gröbner bases [20].

The following procedure produces the first k derivatives of y with respect to x of an algebraic curve $F(x, y)$.

```
> ImDiff:=proc(F,k)
> local f,sf,i,Y,ans;
> if evalb(diff(F,y)=0) then
> ans:=[‘exceptional‘];
> else
> f[0]  := subs(y=y[0],F);
> for i from 1 to k do
> f[i] := TotalDiff(f[i-1],x);
> sf[i]:= subs({y[0]=y,seq(y[j]=Y[j],j=1..(i-1))},f[i]);
> Y[i] := solve(sf[i],y[i]);
> od;
> ans:=[seq(Y[i],i=1..k)];
> fi;
> return ans;
> end:
```

We can then compute the invariants κ^2 and κ_s (see (4.2)) restricted to a curve $X = V(F)$. The procedure will output "SE-exceptional" if the curve is exceptional with respect to the classifying set $\mathcal{I}^{\mathcal{SE}} = \{\kappa^2, \kappa_s\}$.

```
> SEInv:=proc(F)
> local t1,t2,k1,k2,Y,ans;
> Y:=ImDiff(F,3);
> if evalb(Y=[‘exceptional‘]) then
> ans:=[‘SE-exceptional‘];
> else
> if Y[1]^2+1=0 or Y[2]=0 then
> ans:=[‘SE-exceptional‘];
> else
> t1:=Y[2]^2/((Y[1]^2+1)^(3));
> t2:=(Y[1]^2*Y[3]-3*Y[1]*Y[2]^2+Y[3])/(Y[1]^2+1)^3;
> k1:=simplify(factor(t1));
> k2:=simplify(factor(t2));
> ans:=[k1,k2];
> fi;
> fi;
> return ans;
> end:
```

The following procedure computes the size of $\mathrm{Sym}(X, \mathcal{SE}(2))$.

```
> SESymSize:=proc(F)
> local F1,eq,J1,J2,ans;
> F1:=expand(eval(F,[x=c*x-s*y+a,y=s*x+c*y+b]));
> eq:=F-alpha*F1;
> J1:=<Coefficients(eq,x,y),c^2+s^2-1>;
> if evalb(IsRadical(J1)) then
> ans:=NumberOfSolutions(J1);
> else
> J2:=Radical(J1);
> ans:=NumberOfSolutions(J2);
> fi;
> return ans;
> end:
```

Putting these together we can compute the signature polynomial S_X for a curve $X = V(F)$ under the action of $\mathcal{SE}(2)$. If the curve is reducible, $\mathcal{I}^{\mathcal{SE}}$-exceptional, or has infinite symmetry group, the signature polynomial for X is not defined. As a result the procedure will terminate and output the reason for terminating.

```
> SESig:=proc(F)
> local K,K1,K2,Q,q,eq1,eq2,eq3,J,S,SS,ans;
> if evalb(evala(AIrreduc(F))=false) then
> ans:=‘Curve is reducible‘;
> else
> K:=SEInv(F);
> if evalb(K=[‘SE-exceptional‘]) then
> ans:=‘Curve is SE-exceptional‘;
> else
> SS:=SESymSize(F);
> if evalb(SS=infinity) then
> ans:=‘Zero Dimensional Signature‘;
> else
> K1:=K[1];
> K2:=K[2];
> Q:=Generators(Radical(<lcm(denom(K1),denom(K2))>));
> q:=Q[1];
> eq1:=denom(K1)*kappa[1]-numer(K1);
> eq2:=denom(K2)*kappa[2]-numer(K2);
> eq3:=upsilon*q-1;
> J := <eq1, eq2, eq3, F>;
> S:= Generators(EliminationIdeal(J, kappa[1], kappa[2]));
> ans:=S[1];
> fi;
> fi;
> fi;
> return ans;
> end:
```

A.2 Computing Degree Bounds

The degree formula in (3.10) is useful for proving many of the results in this thesis. However, it is difficult to know whether one has chosen a generic value of $\mathbf{a} = [a_0 : a_1 : a_2]$. In particular the procedures here only work over the real numbers, which are often non-generic with respect to $\mathbb{C}^2$. The bounds on the signature's degree in (3.12) and (3.14), allow one to choose any value of $\mathbf{a}$ to compute these bounds. Often these bounds coincide, allowing one to determine exactly the signature polynomial's degree.

The procedures here to compute these bounds still rely on elimination and Gröbner basis algorithms, but these are mainly performed on zero-dimensional ideals. In practice computing the degree bounds for a signature is much quicker than direct computation of the polynomial. The following determines whether the base locus of the signature map is empty.

```
> SEBaseLocus:=proc(F)
> local K,Q,R1,R2,k,F1,s1,s2,s3,J1,J2,J3,h,ans;
> K:=SEInv(F);
> if evalb(K=[‘SE-exceptional‘]) then
> ans:=‘Curve is SE-exceptional‘;
> else
> Q:=lcm(denom(K[1]),denom(K[2]));
> R1:=(Q)/(denom(K[1]));
> R2:=(Q)/(denom(K[2]));
> k:=max(degree(Q,x,y),degree(numer(K[1])*R1,x,y),degree(numer(K[2])*R2,x,y));
> F1:=Homogenize(F, z, x,y);
> s1:=z^(k-degree(numer(K[1])*R1,x,y))*Homogenize(numer(K[1])*R1, z, x,y);
> s2:=z^(k-degree(numer(K[2])*R2,x,y))*Homogenize(numer(K[2])*R2, z, x,y);
> s3:=z^(k-degree(Q,x,y))*Homogenize(Q, z, x,y);
> J1:=<subs(x=1,F1),subs(x=1,s1),subs(x=1,s2),subs(x=1,s3)>;
> J2:=<subs(y=1,F1),subs(y=1,s1),subs(y=1,s2),subs(y=1,s3)>;
> J3:=<subs(z=1,F1),subs(z=1,s1),subs(z=1,s2),subs(z=1,s3)>;
> h:=[IdealMembership(1,J1),IdealMembership(1,J2),IdealMembership(1,J3)];
> if evalb(h=[true, true, true]) then ans:=true else ans:=false fi;
> fi;
> return ans;
> end:
```

For a particular choice of $\mathbf{a}$ the following computes the degree bounds. The procedure first checks that a signature polynomial is defined. If the base locus is empty, by (3.10), we can compute the signature polynomial's degree exactly. Otherwise the sum of the intersection multiplicity of $V(\mathbf{F})$ and $V(\boldsymbol{\sigma}^*_{\mathbf{a}})$ is computing by saturating $\langle \mathbf{F}, \boldsymbol{\sigma}^*_{\mathbf{a}} \rangle$ by $\langle \boldsymbol{\sigma}_0, \boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2 \rangle$, giving a lower bound. We assume that $\langle \mathbf{F}, \boldsymbol{\sigma}^*_{\mathbf{a}} \rangle$ contains no projective points by genericity of $\mathbf{a}$ and compute $\dim_{\mathbb{C}}(\langle \mathbf{F}, \boldsymbol{\sigma}^*_{\mathbf{a}} \rangle|_{z=1})$. In the event, that this assumption is incorrect, this still provides a lower bound.

The upper bound is computed by estimating $\dim_{\mathbb{C}}(\langle \mathbf{F}, \boldsymbol{\sigma}_0, \boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2 \rangle)$ using different affine slices. Even if the procedure does not successfully compute $\dim_{\mathbb{C}}(\langle \mathbf{F}, \boldsymbol{\sigma}_0, \boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2 \rangle)$, it still produces an upper bound for $\deg(S_X)$.

```
> SEDegBound:=proc(F,a1,a2,a0)
> local P1,P2,K,Q,R1,R2,k,SS,L,F1,s1,s2,s3,xF1,yF1,zF1,lb,ub;
> local zs1,zs2,zs3,ys1,ys2,ys3,xs1,xs2,xs3,J,J1,J2,J3,ans,n1,n2,n3;
> if evalb(evala(AIrreduc(F))=false) then
> ans:=‘Curve is reducible‘;
> else
> K:=SEInv(F);
> if evalb(K=[‘SE-exceptional‘]) then
> ans:=‘Curve is SE-exceptional‘;
> else
> SS:=SESymSize(F);
> if evalb(SS=infinity) then
> ans:=‘Zero Dimensional Signature‘;
> else
> Q:=lcm(denom(K[1]),denom(K[2]));
> R1:=(Q)/(denom(K[1]));
> R2:=(Q)/(denom(K[2]));
> P1:=simplify(numer(K[1])*R1);
> P2:=simplify(numer(K[2])*R2);
> k:=max(degree(Q,x,y),degree(P1,x,y),degree(P2,x,y));
> if evalb(SEBaseLocus(F)=true) then
> ans:=[(k*degree(F,x,y))/(SS), ‘exact‘];
> else
> L:=(a1)*P1+(a2)*P2+(a0)*Q;
> J1:=Saturate(<F,L>,P1);
> J2:=Saturate(<F,L>,P2);
> J3:=Saturate(<F,L>,Q);
> J:=PolynomialIdeals[Intersect](J1,J2,J3);
> F1:=Homogenize(F, z, x,y);
> s1:=z^(k-degree(P1,x,y))*Homogenize(P1, z, x,y);
> s2:=z^(k-degree(P2,x,y))*Homogenize(P2, z, x,y);
> s3:=z^(k-degree(Q,x,y))*Homogenize(Q, z, x,y);
```

```
> zs1:=simplify(subs(z=1,s1));
> zs2:=simplify(subs(z=1,s2))
> zs3:=simplify(subs(z=1,s3))
> ys1:=simplify(subs(y=1,s1))
> ys2:=simplify(subs(y=1,s2))
> ys3:=simplify(subs(y=1,s3))
> xs1:=simplify(subs(x=1,s1))
> xs2:=simplify(subs(x=1,s2))
> xs3:=simplify(subs(x=1,s3))
> xF1:=simplify(subs(z=1,F1))
> yF1:=simplify(subs(y=1,F1))
> zF1:=simplify(subs(z=1,F1))
> n1:=NumberOfSolutions(<zF1,zs1,zs2,zs3>);
> n2:=NumberOfSolutions(<yF1,ys1,ys2,ys3,z^1000>);
> n3:=NumberOfSolutions(<xF1,xs1,xs2,xs3,y^1000,z^1000>);
> lb:=(NumberOfSolutions(J))/(SS);
> ub:=simplify((k*degree(F,x,y)-(n1+n2+n3))/(SS))
> ans:=[lb, `<= Degree <=`, ub];
> fi;
> fi;
> fi;
> fi;
> return ans;
> end:
```

APPENDIX B

Details for Proofs in Section 4.2.1

Here we provide justification for many of the computational claims made in the Section 4.2.1.

B.1 T polynomials and Lemma 4.2.1

We first compute the first n derivatives of y with respect to x in terms of the partial derivatives of $F(x, y)$, and then evaluate each differential polynomial restricted to $F(x, y)$ in terms of those partials. The output of Θ_3 is hidden due to its length.

```
> PDEtools[declare](F(x,y), quiet);
> Y:=ImDiff(F(x,y),3):
> Theta[1]:=Y[1]^2+1;
> Theta[2]:=Y[2];
> Theta[3]:=Y[3]*Theta[1]-3*Y[1]*Theta[2]^2:
```

$$\Theta_1 := \frac{F_x^2 + F_y^2}{F_y^2}$$

$$\Theta_2 := -\frac{F_x^2 F_{y,y} - 2F_{x,y}F_x F_y + F_{x,x}F_y^2}{F_y^3}$$

In each case we can write the differential polynomials as a polynomial in partials of $F(x, y)$ over F_y^k for some $k \in \mathbb{Z}_+$.

```
> T[1]:=numer(Theta[1]);
> denom(Theta[1]);
> T[2]:=numer(Theta[2]);
> denom(Theta[2]);
```

$$T_1 := F_x^2 + F_y^2$$

$$F_y$$

$$T_2 := -F_x^2 F_{y,y} - 2F_{x,y}F_x F_y + F_{x,x}F_y^2$$

$$F_y^3$$

In the case of Θ_3, after some simplification the power of F_y drops.

```
> T[1]:=numer(Theta[1]);
> denom(Theta[3]);
> Theta[3]:=simplify(Theta[3]):
> denom(Theta[3]);
```

$$F_y^7$$

$$F_y^6$$

We can similarly compute the rest of the differential functions below. The output of each function is hidden, but we can still determine see the power of F_y in each denominator after simplification.

```
> Theta[4]:=expand(3*Y[4]*Y[2]-5*Y[3]^2):
> denom(Theta[4]);
```

$$F_y^8$$

```
> Theta[5]:=expand(9*Y[5]*Y[2]^2-45*Y[4]*Y[3]*Y[2]+40*Y[3]^3):
> denom(Theta[5]);
```

$$F_y^{12}$$

```
> Theta[6]:=expand(9*Y[6]*Y[2]^3-63*Y[5]*Y[3]*Y[2]^2-45*Y[4]^2*Y[2]^2
> +255*Y[4]*Y[3]^2*Y[2]-160*Y[3]^4):
> denom(Theta[6]);
```

$$F_y^{16}$$

```
> Theta[7]:=(9/2)*expand(18*Y[7]*Y[2]^4*(9*Y[5]*Y[2]^2
> -45*Y[4]*Y[3]*Y[2]+40*Y[3]^3)-189*Y[6]^2*Y[2]^6
> +126*Y[6]*Y[2]^4*(9*Y[5]*Y[3]*Y[2]+15*Y[4]^2*Y[2]-25*Y[4]*Y[3]^2)
> -189*Y[5]^2*Y[2]^4*(4*Y[3]^2+15*Y[2]*Y[4]+210*Y[5]*Y[3]*Y[2]^2
> *(63*Y[4]^2*Y[2]^2-60*Y[4]*Y[3]^2*Y[2]+32*Y[3]^4)
> -525*Y[4]*Y[2]*(9*Y[4]^3*Y[2]^3+15*Y[4]^2*Y[3]^2*Y[2]^2
> -60*Y[4]*Y[3]^4*Y[2]+64*Y[3]^6)+ 11200*Y[3]^8):
> denom(Theta[7]);
```

$$2F_y^{32}$$

```
> Theta[8]:=expand(243*Y[2]^4/(2)*(2*Y[8]*Y[2]*(9*Y[5]*Y[2]^2
> -45*Y[4]*Y[3]*Y[2]+40*Y[3]^3)^2-8*Y[7]*(9*Y[5]*Y[2]^2
> -45*Y[4]*Y[3]*Y[2]+40*Y[3]^3)*(9*Y[6]*Y[2]^3
> -36*Y[5]*Y[3]*Y[2]^2-45*Y[4]^2*Y[2]^2+120*Y[4]*Y[3]^2*Y[2]
> -40*Y[3]^4)+504*Y[6]^3*Y[2]^5
> -504*Y[6]^2*Y[2]^3*(9*Y[5]*Y[3]*Y[2]+15*Y[4]^2*Y[2]
> -25*Y[4]*Y[3]^2)+28*Y[6]*(432*Y[5]^2*Y[3]^2*Y[2]^3
> +243*Y[5]^2*Y[4]*Y[2]^4-1800*Y[5]*Y[4]*Y[3]^3*Y[2]^2
> -240*Y[5]*Y[3]^5*Y[2]+540*Y[5]*Y[4]^2*Y[3]*Y[2]^3
> +6600*Y[4]^2*Y[3]^4*Y[2]-2000*Y[4]*Y[3]^6
> -5175*Y[4]^3*Y[3]^2*Y[2]^2+1350*Y[4]^4*Y[2]^3)
> -2835*Y[5]^4*Y[2]^4+252*Y[5]^3*Y[3]*Y[2]^2
> *(9*Y[4]*Y[2]-136*Y[3]^2)-35840*Y[5]^2*Y[3]^6
> -630*Y[5]^2*Y[4]*Y[2]*(69*Y[4]^2*Y[2]^2-160*Y[3]^4
> -153*Y[4]*Y[3]^2*Y[2]+2100*Y[5]*Y[4]^2*Y[3]
> *(72*Y[3]^4+63*Y[4]^2*Y[2]^2-193*Y[4]*Y[3]^2*Y[2])
> -7875*Y[4]^4*(8*Y[4]^2*Y[2]^2-22*Y[4]*Y[3]^2*Y[2]
> +9*Y[3]^4))):
> denom(Theta[8]);
```

$$2F_y^{48}$$

```
> Theta[9]:=expand(Y[1]^4*Y[4]-10*Y[1]^3*Y[2]*Y[3]+(15*Y[2]^3+2*Y[4])
> *Y[1]^2-10*Y[1]*Y[2]*Y[3]+Y[4]):
> denom(Theta[9]);
```

$$F_y^9$$

B.2 Details for Lemma 4.2.3

The command

```
> DerivOrigin
```

first computes each partial derivative of $F(x, y)$ at the origin. It then finds the derivative of y with respect to x of F at the origin using the partial derivative representation. We can then evaluate the polynomial T_1 obtained from F at the origin.

```
> T1Origin:=proc(F)
> local FY, Fy, Y, M1, D1;
> Y:=DerivOrigin(F);
> Fy :=diff(F, y);
> FY:= subs(x=0,y=0,Fy);
> D1:=Y[1]^2+1;
> M1:=FY^2*(D1);
> return(simplify(M1))
> end:
```

The commands to evaluate T_i for $i = 2, \ldots, 9$ are defined similarly. First we define an arbitrary second degree curve that contains the origin.

```
> F:=a[1,0]*x+a[0,1]*y+sum(a[i,2-i]*x^i*y^(2-i),i=0..2);
```

$$F := a_{2,0}x^2 + a_{1,1}xy + a_{0,2}y^2 + a_{1,0}x + a_{0,1}y$$

Since T_1 and T_2 depend on partials of order ≤ 2, the polynomials $T_1(0,0)$ and $T_2(0,0)$ only depend on coefficients $a_{i,j}$ where $i + j \leq 2$. Thus we can compute $T_1(0,0)$ and $T_2(0,0)$ and see that they do not share a common factor for a curve of any degree.

```
> T[1]:=T1Origin(F);
> T[2]:=T2Origin(F);
> gcd(T[1],T[2]);
```

$$T_1 := {a_{0,1}}^2 + {a_{1,0}}^2$$
$$T_2 := -2\,a_{2,0}{a_{0,1}}^2 + 2\,a_{1,1}a_{1,0}a_{0,1} - 2\,{a_{1,0}}^2 a_{0,2}$$
$$1$$

We can also do this for the other pairs of polynomials discussed in Lemma 4.2.3. The computations are not included here due to their redundancy and length.

B.3 Details for Lemma 4.2.6

Here we evaluate the differential functions Θ on truncations of Laurent series, representing points at infinity on a curve $F(x, y)$, and then compute their valuation. The code first outputs the coefficient of the lowest degree term of the series and then its degree.

```
> xt:=(1/t):
> yt:=a[0]/t+a[1]+sum(a[i+1]*t^i,i=1..60):
> y[1]:=expand((diff(yt,t))/(diff(xt,t))):
> y[2]:=expand((diff(y[1],t))/(diff(xt,t))):
> y[3]:=expand((diff(y[2],t))/(diff(xt,t))):
> y[4]:=expand((diff(y[3],t))/(diff(xt,t))):
> y[5]:=expand((diff(y[4],t))/(diff(xt,t))):
> y[6]:=expand((diff(y[5],t))/(diff(xt,t))):
> y[7]:=expand((diff(y[6],t))/(diff(xt,t))):
> y[8]:=expand((diff(y[7],t))/(diff(xt,t))):
> Theta1:=expand(y[1]^2+1):
> tcoeff(Theta1,[t],'ValTheta1');
> ValTheta1;
```

$$a_0^2 + 1$$
$$1$$

```
> Theta2:=expand(y[2]):
> Theta3:=expand(y[3]*Theta1-3*y[1]*y[2]^2):
> Theta4:=expand(3*y[4]*y[2]-5*y[3]^2):
> tcoeff(Theta2,[t],'ValTheta2');
> ValTheta2;
> tcoeff(Theta3,[t],'ValTheta3');
> ValTheta3;
> tcoeff(Theta4,[t],'ValTheta4');
> ValTheta4;
```

$$2a_2$$
$$t^3$$
$$-6a_0^2a_2 - 6a_2$$
$$t^4$$
$$-36a_2^2$$
$$t^8$$

The following command truncates the series at a given power of t. Note that for each expression the lowest degree term must be of non-negative degree. Some coefficients are hidden due to length.

```
> Truncate:=proc(F,n)
> local i,c,TF;
> for i from 0 to n do
> c[i]:=coeff(F,t,i):
> od;
> TF:=sum(c[j]*t^j,j=0..n);
> return(TF);
> end:
> Theta9:=expand(Truncate(y[1]^4*y[4]-10*y[1]^3*y[2]*y[3]+(15*y[2]^3
> +2*y[4])*y[1]^2-10*y[1]*y[2]*y[3]+y[4],40)):
> Theta5:=expand(Truncate(9*y[5]*y[2]^2-45*y[4]*y[3]*y[2]+40*y[3]^3,40)):
> Theta6:=expand(Truncate(9*y[6]*y[2]^3-63*y[5]*y[3]*y[2]^2
> -45*y[4]^2*y[2]^2+255*y[4]*y[3]^2*y[2]-160*y[3]^4,40)):
```

```
> Theta7:=expand(Truncate((9/2)*(18*y[7]*y[2]^4
> *(9*y[5]*y[2]^2-45*y[4]*y[3]*y[2]
> +40*y[3]^3)-189*y[6]^2*y[2]^6+126*y[6]*y[2]^4
> *(9*y[5]*y[3]*y[2]+15*y[4]^2*y[2]-25*y[4]*y[3]^2)
> -189*y[5]^2*y[2]^4*(4*y[3]^2+15*y[2]*y[4])
> +210*y[5]*y[3]*y[2]^2*(63*y[4]^2*y[2]^2
> -60*y[4]*y[3]^2*y[2]+32*y[3]^4)-525*y[4]*y[2]
> *(9*y[4]^3*y[2]^3+15*y[4]^2*y[3]^2*y[2]^2
> -60*y[4]*y[3]^4*y[2]+64*y[3]^6)+ 11200*y[3]^8),40)):
> Theta8:=expand(Truncate((243*y[2]^4/(2)
> *(2*y[8]*y[2]*(9*y[5]*y[2]^2-45*y[4]*y[3]*y[2]
> +40*y[3]^3)^2-8*y[7]*(9*y[5]*y[2]^2-45*y[4]*y[3]*y[2]
> +40*y[3]^3)*(9*y[6]*y[2]^3-36*y[5]*y[3]*y[2]^2
> -45*y[4]^2*y[2]^2+120*y[4]*y[3]^2*y[2]-40*y[3]^4)
> +504*y[6]^3*y[2]^5-504*y[6]^2*y[2]^3
> *(9*y[5]*y[3]*y[2]+15*y[4]^2*y[2]-25*y[4]*y[3]^2)
> +28*y[6]*(432*y[5]^2*y[3]^2*y[2]^3+243*y[5]^2*y[4]*y[2]^4
> -1800*y[5]*y[4]*y[3]^3*y[2]^2-240*y[5]*y[3]^5*y[2]
> +540*y[5]*y[4]^2*y[3]*y[2]^3+6600*y[4]^2*y[3]^4*y[2]
> -2000*y[4]*y[3]^6-5175*y[4]^3*y[3]^2*y[2]^2
> +1350*y[4]^4*y[2]^3)-2835*y[5]^4*y[2]^4
> +252*y[5]^3*y[3]*y[2]^2*(9*y[4]*y[2]-136*y[3]^2)
> -35840*y[5]^2*y[3]^6-630*y[5]^2*y[4]*y[2]
> *(69*y[4]^2*y[2]^2-160*y[3]^4-153*y[4]*y[3]^2*y[2])
> +2100*y[5]*y[4]^2*y[3]*(72*y[3]^4+63*y[4]^2*y[2]^2
> -193*y[4]*y[3]^2*y[2])-7875*y[4]^4*(8*y[4]^2*y[2]^2
> -22*y[4]*y[3]^2*y[2]+9*y[3]^4))),60)):
> tcoeff(Theta5,[t],'ValTheta5');
> ValTheta5;
> tcoeff(Theta6,[t],'ValTheta6');
> ValTheta6;
> tcoeff(Theta7,[t],'ValTheta7'):
> ValTheta7;
> tcoeff(Theta8,[t],'ValTheta8'):
> ValTheta8;
> tcoeff(Theta9,[t],'ValTheta9');
> ValTheta9;
```

$$-4320a_5a_2^2 + 12960a_4a_2a_3 - 8640a_3^3$$

$$t^{15}$$

$$25920a_2^3a_5 - 77760a_2^2a_3a_4 + 51840a_2a_3^3$$

$$t^{19}$$

$$-36a_2^2$$

$$t^8$$

$$t^{40}$$

$$t^{60}$$

$$24a_0^4a_2 + 48a_0^2a_2 + 24a_2$$

$$t^5$$

APPENDIX C

Fermat Curve Computations

This appendix contains details for the proofs of Proposition 4.3.2 and Theorem 4.3.3.

C.1 Affine

For $3 \leq d \leq 7$ we compute the signature polynomial for the Fermat curves X_d under the action of $\mathcal{A}(2)$ directly.

```
> F:=x^3+y^3+1;
> ASig(F);
```

$$F := x^3 + y^3 + 1$$

$$25\,{\kappa_1}^2 - 300\,\kappa_1\kappa_2 + 900\,{\kappa_2}^2 + 820\,\kappa_1 + 960\,\kappa_2 + 256$$

```
> F:=x^4+y^4+1;
> ASig(F);
```

$$F := x^4 + y^4 + 1$$

$$13720\,{\kappa_2}^3 + 49\,{\kappa_1}^2 - 13230\,\kappa_1\kappa_2 + 176400\,{\kappa_2}^2 + 76300\,\kappa_1 + 231000\,\kappa_2 + 80000$$

```
> F:=x^5+y^5+1;
> ASig(F);
```

$$F := x^5 + y^5 + 1$$

$$225\,{\kappa_2}^3 + 1485\,{\kappa_2}^2 + 343\,\kappa_1 + 1944\,\kappa_2 + 720$$

```
> F:=x^6+y^6+1;
> ASig(F);
```

$$F := x^6 + y^6 + 1$$

$$2012472\,{\kappa_2}^3 - 121\,{\kappa_1}^2 + 193116\,\kappa_1\kappa_2 + 10245312\,{\kappa_2}^2 + 1431584\,\kappa_1 + 13039488\,\kappa_2 + 4917248$$

```
> F:=x^7+y^7+1;
> ASig(F);
```

$$F := x^7 + y^7 + 1$$

$$8612240\,{\kappa_2}^3 - 1183\,{\kappa_1}^2 + 851760\,\kappa_1\kappa_2 + 38329200\,{\kappa_2}^2 + 3551600\,\kappa_1 + 47424000\,\kappa_2 + 17920000$$

The following computes the classifying invariants for $\mathcal{A}(2)$ (see (4.3)) restricted to the curve $\overline{F} = x^6a + y^6b + 1$.

```
> F:=x^d+y^d+1:
> YY:=ImDiff(F,6):
> Y:=[subs(x^d=x^6*a,y^d=y^6*b,YY[1]),subs(x^d=x^6*a,y^d=y^6*b,YY[2]),
> subs(x^d=x^6*a,y^d=y^6*b,YY[3]),subs(x^d=x^6*a,y^d=y^6*b,YY[4]),
> subs(x^d=x^6*a,y^d=y^6*b,YY[5]),subs(x^d=x^6*a,y^d=y^6*b,YY[6])]:
> Delta1:=simplify(3*Y[4]*Y[2]-5*Y[3]^2):
> Delta2:=simplify(9*Y[5]*Y[2]^2-45*Y[4]*Y[3]*Y[2]+40*Y[3]^3):
> K1:= Delta2^2/Delta1^3:
> K2:= 1/Delta1^2*(9*Y[6]*Y[2]^3-63*Y[5]*Y[3]*Y[2]^2
> -45*Y[4]^2*Y[2]^2+255*Y[4]*Y[3]^2*Y[2]-160*Y[3]^4):
> Inv:=[simplify(factor(K1)),simplify(factor(K2))]:
```

By canceling common factors and clearing denominators, we can construct three polynomials $s_i = \overline{\boldsymbol{\sigma}}_i \in \mathbb{Q}[x, y, a, b, d]$, $i = 0, 1, 2$ such that $\overline{\boldsymbol{\sigma}}_i$ evaluated at $a = x^{d-6}, b = y^{d-6}$ gives $\boldsymbol{\sigma}_i$ where $\boldsymbol{\sigma} = [\boldsymbol{\sigma}_0, \boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2]$ is a projective extension of $\boldsymbol{\sigma}^{\mathcal{A}}_{X_d}$.

```
> s[0]:=lcm(denom(Inv[1]),denom(Inv[2]));
> s[1]:=simplify(numer(Inv[1])*(s0/denom(Inv[1])));
> s[2]:=simplify(numer(Inv[2])*(s0/denom(Inv[2])));
```

$$s_0 := (2\,d-1)\left(x^{12}a^2d + x^6ay^6bd + y^{12}b^2d - 2\,x^{12}a^2 - 5\,x^6ay^6b - 2\,y^{12}b^2\right)^3$$

$$s_1 := -2\,\frac{\left(x^6a - y^6b\right)^2\left(x^6a + 2\,y^6b\right)^2(d-2)^2(1+d)^2\left(x^6a + 1/2\,y^6b\right)^2}{(d-1/2)\left(x^{12}(d-2)a^2 + bx^6y^6(d-5)a + b^2y^{12}(d-2)\right)^3}$$

$$s_2 := -\frac{(1+d)(d-2)\left(x^{24}(1+d)a^4 + 2\,b(d+1/4)x^{18}y^6a^3 + 3\,b^2x^{12}y^{12}(d-1)a^2 + 2\,b^3(d+1/4)x^6y^{18}a + b^4y^{24}(1+d)\right)}{(d-1/2)\left(x^{12}(d-2)a^2 + bx^6y^6(d-5)a + b^2y^{12}(d-2)\right)^2}$$

The ideal $J1$ below represents the ideal of affine points $[1:p] \in V(F_d)$ in the base locus of $\boldsymbol{\sigma}$.

```
> J1:=<x^6*a+y^6*b+1,s0,s1,s2>:
> B:=Groebner[Basis](J,plex(x,y,a,b,d)):
> factor(B[1]);
```

$$d^3\,(d-3)\,(d-2)^2$$

The ideal $J2$ below represents the ideal of points of the form $[0:p] \in V(F_d)$ in the base locus of $\boldsymbol{\sigma}$.

```
> J2:=<x^6*a+y^6*b,s0,s1,s2>:
> B:=Groebner[Basis](J,plex(x,y,a,b,d));
> factor(B[1]);
```

$$b^6y^{36}\,(1+d)^2$$

C.2 Projective

For $3 \leq d \leq 7$ we compute the signature polynomial for the Fermat curves X_d under the action of $\mathcal{PGL}(3)$ directly.

```
> F:=x^3+y^3+1;
> PSig(F);
```

$$F := x^3 + y^3 + 1$$

$$4410000\,{\kappa_2}^4 + 53760000\,\kappa_1{\kappa_2}^2 + 333396000\,{\kappa_2}^3 + 163840000\,{\kappa_1}^2 -$$

$$677376000\,\kappa_1\kappa_2 + 9451776600\,{\kappa_2}^2 - 32006016000\,\kappa_1 + 119092385160\,\kappa_2 + 562711519881$$

```
> F:=x^4+y^4+1;
> PSig(F);
```

$$F := x^4 + y^4 + 1$$

$$18974430720000\,{\kappa_2}^4 + 231307345920000\,\kappa_1{\kappa_2}^2 + 1015224011424000\,{\kappa_2}^3$$
$$+704936673280000\,{\kappa_1}^2 - 2153990651904000\,\kappa_1\kappa_2 + 20367401451742800\,{\kappa_2}^2$$
$$-66627150406992000\,\kappa_1 + 181582957508150835\,\kappa_2 + 607005886527247077$$

```
> F:=x^5+y^5+1;
> PSig(F);
```

$$F := x^5 + y^5 + 1$$

$$7938000\,{\kappa_2}^4 + 96768000\,\kappa_1{\kappa_2}^2 + 370851600\,{\kappa_2}^3 + 294912000\,{\kappa_1}^2$$
$$-812851200\,\kappa_1\kappa_2 + 6494801040\,{\kappa_2}^2 - 20705345920\,\kappa_1 + 50534548092\,\kappa_2 + 147392431935$$

```
> F:=x^6+y^6+1;
> PSig(F);
```

$$F := x^6 + y^6 + 1$$

$$1777949697097728\,{\kappa_2}^4 + 21674053450334208\,\kappa_1{\kappa_2}^2 + 77456469265781760\,{\kappa_2}^3$$
$$+66054258134351872\,{\kappa_1}^2 - 173895072627032064\,\kappa_1\kappa_2$$
$$+1264620282724814400\,{\kappa_2}^2 - 3956041407609156096\,\kappa_1$$
$$+9170632023542797500\,\kappa_2 + 24921490271770524375$$

```
> F:=x^7+y^7+1;
> PSig(F);
```

$$F := x^7 + y^7 + 1$$

$$302415578010000\,{\kappa_2}^4 + 3686589903360000\,\kappa_1{\kappa_2}^2 + 12638217612384000\,{\kappa_2}^3$$
$$+11235321610240000\,{\kappa_1}^2 - 28892563225344000\,\kappa_1\kappa_2 + 197891393481873000\,{\kappa_2}^2$$
$$-610304534673724800\,\kappa_1 + 1375912588829959440\,\kappa_2 + 3583987695327269349$$

The following computes the classifying invariants for $\mathcal{PGL}(3)$ (see (4.3)) restricted to the curve $\overline{F} = x^6a + y^6b + 1$.

```
> YY:=ImDiff(F,8):
> Y:=[subs(x^d=x^8*a,y^d=y^8*b,YY[1]),subs(x^d=x^8*a,y^d=y^8*b,YY[2]),
> subs(x^d=x^8*a,y^d=y^8*b,YY[3]),subs(x^d=x^8*a,y^d=y^8*b,YY[4]),
> subs(x^d=x^8*a,y^d=y^8*b,YY[5]),subs(x^d=x^8*a,y^d=y^8*b,YY[6]),
> subs(x^d=x^8*a,y^d=y^8*b,YY[7]),subs(x^d=x^8*a,y^d=y^8*b,YY[8])]:
> Delta2:=simplify(9*Y[5]*Y[2]^2-45*Y[4]*Y[3]*Y[2]+40*Y[3]^3):
> K1:= 729/(8*Delta2^8)*(18*Y[7]*Y[2]^4*Delta2-189*Y[6]^2*Y[2]^6+126*Y[6]*Y[2]^4
> *(9*Y[5]*Y[3]*Y[2]+15*Y[4]^2*Y[2]-25*Y[4]*Y[3]^2)-189*Y[5]^2*Y[2]^4
> *(4*Y[3]^2+15*Y[2]*Y[4]+210*Y[5]*Y[3]*Y[2]^2*(63*Y[4]^2*Y[2]^2
> -60*Y[4]*Y[3]^2*Y[2]+32*Y[3]^4)-525*Y[4]*Y[2]*(9*Y[4]^3*Y[2]^3
> +15*Y[4]^2*Y[3]^2*Y[2]^2-60*Y[4]*Y[3]^4*Y[2]+64*Y[3]^6)+ 11200*Y[3]^8)^3:
> K2:=243*Y[2]^4/(2*Delta2^4)*(2*Y[8]*Y[2]*Delta2^2-8*Y[7]*Delta2
> *(9*Y[6]*Y[2]^3-36*Y[5]*Y[3]*Y[2]^2-45*Y[4]^2*Y[2]^2
> +120*Y[4]*Y[3]^2*Y[2]-40*Y[3]^4)+504*Y[6]^3*Y[2]^5-504*Y[6]^2*Y[2]^3
> *(9*Y[5]*Y[3]*Y[2]+15*Y[4]^2*Y[2]-25*Y[4]*Y[3]^2)+28*Y[6]
> *(432*Y[5]^2*Y[3]^2*Y[2]^3+243*Y[5]^2*Y[4]*Y[2]^4-1800*Y[5]*Y[4]*Y[3]^3*Y[2]^2
> -240*Y[5]*Y[3]^5*Y[2]+540*Y[5]*Y[4]^2*Y[3]*Y[2]^3+6600*Y[4]^2*Y[3]^4*Y[2]
> -2000*Y[4]*Y[3]^6-5175*Y[4]^3*Y[3]^2*Y[2]^2+1350*Y[4]^4*Y[2]^3)
> -2835*Y[5]^4*Y[2]^4+252*Y[5]^3*Y[3]*Y[2]^2*(9*Y[4]*Y[2]-136*Y[3]^2)
> -35840*Y[5]^2*Y[3]^6-630*Y[5]^2*Y[4]*Y[2]*(69*Y[4]^2*Y[2]^2
> -160*Y[3]^4-153*Y[4]*Y[3]^2*Y[2]+2100*Y[5]*Y[4]^2*Y[3]
> *(72*Y[3]^4+63*Y[4]^2*Y[2]^2-193*Y[4]*Y[3]^2*Y[2])-7875*Y[4]^4
> *(8*Y[4]^2*Y[2]^2-22*Y[4]*Y[3]^2*Y[2]+9*Y[3]^4)):
> Inv:=[simplify(factor(K1)),simplify(factor(K2))]:
```

By canceling common factors and clearing denominators, we can construct three polynomials $s_i = \overline{\boldsymbol{\sigma}}_i \in \mathbb{Q}[x, y, a, b, d]$, $i = 0, 1, 2$ such that $\overline{\boldsymbol{\sigma}}_i$ evaluated at $a = x^{d-8}, b = y^{d-8}$ gives $\boldsymbol{\sigma}_i$ where $\boldsymbol{\sigma} = [\boldsymbol{\sigma}_0, \boldsymbol{\sigma}_1, \boldsymbol{\sigma}_2]$ is a projective extension of $\boldsymbol{\sigma}^{\mathcal{P}}_{X_d}$.

```
> s[0]:=lcm(denom(Inv[1]),denom(Inv[2]));
> s[1]:=simplify(numer(Inv[1])*(s0/denom(Inv[1])));
> s[2]:=simplify(numer(Inv[2])*(s0/denom(Inv[2])));
```

$$
\begin{aligned}
s_0 :=& 8\left(2x^8a+y^8b\right)^8(d-2)^2\left(x^8a+2y^8b\right)^8(1+d)^2(2d-1)^2\left(x^8a-y^8b\right)^8\\
s_1 :=& \frac{729\left(x^{16}a^2+x^8ay^8b+y^{16}b^2\right)^3}{128\left(x^8a+1/2\,y^8b\right)^8\left(x^8a-y^8b\right)^8(1+d)^2\left(x^8a+2y^8b\right)^8(d-2)^2(d-1/2)^2}\\
&\left(x^{48}\left(d^2-d+1\right)a^6+3bx^{40}y^8\left(d^2-d+1\right)a^5-\frac{33b^2\left(d^2-d/22+1/22\right)x^{32}y^{16}a^4}{2}\right.\\
&-38b^3\left(d^2-\frac{13d}{76}+\frac{13}{76}\right)x^{24}y^{24}a^3-\frac{33b^4\left(d^2-d/22+1/22\right)x^{16}y^{32}a^2}{2}\\
&\left.+3b^5x^8y^{40}\left(d^2-d+1\right)a+b^6y^{48}\left(d^2-d+1\right)\right)^3\\
s_2 :=& -\frac{729db^2\left(x^8a+y^8b\right)^2x^{16}y^{16}a^2}{8\left(x^8a+1/2\,y^8b\right)^4\left(x^8a-y^8b\right)^4(1+d)\left(x^8a+2y^8b\right)^4(d-2)(d-1/2)}\\
&\left((d-1/3)(d+1/2)x^{48}a^6+3b(d-1/3)(d+1/2)x^{40}y^8a^5+\frac{39a^4b^2x^{32}y^{16}}{4}\right.\\
&\left(d^2-\frac{d}{78}+\frac{1}{78}\right)+\frac{29a^3b^3x^{24}y^{24}}{2}\left(d^2-\frac{13d}{174}+\frac{13}{174}\right)+\frac{39a^2b^4x^{16}y^{32}}{4}\\
&\left.\left(d^2-\frac{d}{78}+\frac{1}{78}\right)+3b^5(d-1/3)(d+1/2)x^8y^{40}a+b^6(d-1/3)(d+1/2)y^{48}\right)
\end{aligned}
$$

The ideal $J1$ below represents the ideal of affine points $[1:p]\in V(F_d)$ in the base locus of $\boldsymbol{\sigma}$. Thus this ideal is empty for $d\geq 3$.

```
> J1:=<x^8*a+y^8*b+1,s0,s1,s2>:
> B:=Groebner[Basis](J,plex(x,y,a,b,d)):
> factor(B[1]);
```

$$d^9(d-2)(2*d-1)(1+d)$$

The ideal $J2$ below represents the ideal of points of the form $[0:p]\in V(F_d)$ in the base locus of $\boldsymbol{\sigma}$. We can see that since ideal is empty, since for $[0:p_1:p_2]\in V(F_d)$, $p_1,p_2\neq 0$.

```
> J2:=<x^8*a+y^8*b,s0,s1,s2>:
> B:=Groebner[Basis](J,plex(x,y,a,b,d));
```