Computing rational invariants characterizing polynomials up to orthogonal transformations

Paul Görlach

Born February 10, 1992 in Berlin, Germany

Master's Thesis Computer Science

March 22, 2017

Advisor: Prof. Dr. Andreas Weber
INSTITUTE OF COMPUTER SCIENCE II, UNIVERSITY OF BONN

Second Advisor: Dr. Evelyne Hubert
INRIA MÉDITERRANÉE

MATHEMATISCH-NATURWISSENSCHAFTLICHE FAKULTÄT DER
RHEINISCHEN FRIEDRICH-WILHELMS-UNIVERSITÄT BONN

Contents

Abstract

This thesis is centered around the following question:

Question. *When do two polynomial functions $f, g\colon \mathbb{R}^n \to \mathbb{R}$ agree up to an orthogonal transformation, i.e. $f = g \circ \varphi$ for some $\varphi \in O(n)$?*

In this thesis, we restrict our treatment to the case of homogeneous polynomials of even degree.

From a perspective of Invariant Theory, the above question can be answered by evaluating certain algebraic expressions in terms of the coefficients of a polynomial (called *invariants*) which describe the polynomial function up to orthogonal transformations. Classically, these algebraic expressions are *polynomial expressions* in terms of the coefficients, and the problems of determining them, algorithmically evaluating them and further connected questions quickly become computationally infeasible as the degree of the polynomial function increases.

We study this problem, but allowing the invariants to be *rational expressions* instead of only polynomial expressions. This additional flexibility – coming at the expense of excluding cases where certain denominators vanish – allows us to describe a minimal complete set of rational invariants in the geometrically most important cases of dimension $n = 2$ and $n = 3$. Furthermore, we describe algorithmic solutions for related questions of evaluation, rewriting and reconstruction.

The results of this thesis can find applications in describing and analyzing the geometric shape of curves and surfaces in a coordinate-free manner. Specifically, this study was motivated by possible applications in Neuroimaging, where invariants may provide an important preprocessing step for analyzing Diffusion Magnetic Resonance measurements by methods of Machine Learning and Statistical Testing.

CHAPTER 1

Introduction

We start out in Section 1.1 by giving a motivation from a geometric viewpoint for the underlying problem of this thesis. In Section 1.2 we describe how the problem naturally occurs in a Neuroimaging context. Formal definitions and a precise problem statement will be delayed to Chapter 2.

1.1. Geometric motivation

Describing, encoding and manipulating geometric objects such as curves or surfaces is the basis for many algorithmic approaches from different fields in Computer Science. A fundamental question in this context is: *When do two geometric objects have the same shape?* Depending on the geometric objects under consideration and the interpretation of what it means to have the "same shape", this leads to different algorithmic problems. This thesis is concerned with one of those possible viewpoints.

Say, we are interested in closed curves in the two-dimensional plane. These may be described in different ways, e.g. by sampling points on the curve and interpolating (with some convention for the interpolation scheme). The description we are interested in in this thesis, is modeling a closed curve as a deformation of a circle in the following sense: For any continuous function $f\colon S^1 \to \mathbb{R}$ (where $S^1 := \{p = (x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$ is the unit circle), we consider the curve

$$C := \{f(p) \cdot p \in \mathbb{R}^2 \mid p \in S^1\} \subset \mathbb{R}^2,$$

i.e. for each point on the unit circle we rescale its distance to the origin according to the function f. For example, the curve described by a constant function $f \equiv r$ (for some $r \in \mathbb{R}$) is the circle with radius $|r|$ centered at the origin. As f takes on more general functions, a large variety of different curves can be described.

We will focus on curves which are symmetric with respect to the origin – this corresponds to imposing the property

$$f(p) = f(-p) \quad \forall p \in S^1 \tag{1.1.1}$$

on the describing function $f\colon S^1 \to \mathbb{R}$.

Since the unit circle $S^1 \subset \mathbb{R}^2$ is a compact set, the Stone–Weierstraß Theorem implies that an arbitrary continuous functions $S^1 \to \mathbb{R}$ can be approximated arbitrarily well by a polynomial function, i.e. by a function $f\colon S^1 \to \mathbb{R}$ of the form

$$f(x, y) = \sum_{i+j \leq k} a_{i,j} x^i y^j.$$

Because of this approximation property, we restrict to the case that $f\colon S^1 \to \mathbb{R}$ is such a polynomial function. Note that the symmetry assumption (1.1.1) is fullfilled if and only $a_{i,j} = 0$ whenever $i + j$ is odd, in other words, f must only consist of even-degree terms. We can rewrite f in such a way that all its monomials are of the same degree, by multiplying monomials of smaller degree with a suitable power of $x^2 + y^2$ (which of course does not change the values of f, since $x^2 + y^2 = 1$ for all points (x, y) on the circle).

To conclude, we model curves which are symmetric with respect to the origin by a function $f\colon S^1 \to \mathbb{R}$ given by

$$f(x, y) = \sum_{i=0}^{2d} a_i x^{2d-i} y^i,$$

where the *degree* $2d$ is an even number.

Note that the description of such a modeled curve can then be encoded *exactly* by simply storing the $2d + 1$ numbers $a_0, a_1, \ldots, a_{2d} \in \mathbb{R}$.

However, from such a numerical encoding of a curve as $2d + 1$ coefficients a_i of the defining polynomial, it is not immediately apparent when two curves have equal geometric shapes, only differing by their embedding in the coordinate system. As an example, Figure 1.1 depicts the two curves C_1 and C_2 defined by

$$\begin{aligned} f_1(x, y) &:= 1250x^4 + 1250x^3y - 625x^2y^2 + 1875y^4 \text{ and} \\ f_2(x, y) &:= 1002x^4 + 906x^3y + 5063x^2y^2 - 56xy^3 + 227y^4, \end{aligned}$$

respectively, whose numerical description in terms of coefficients look very distinct, but whose shapes look very similar. Indeed, it can be checked that C_2 arises from C_1 by applying the rotation matrix

$$\begin{pmatrix} 3/5 & 4/5 \\ -4/5 & 3/5 \end{pmatrix}.$$

In general, we want to consider curves to be of the same shape if they differ by an orthogonal transformation.

The question which arises is: *How can we (algorithmically) decide whether two curves only differ by an orthogonal transformation, only by looking at the coefficients of their defining polynomial?*

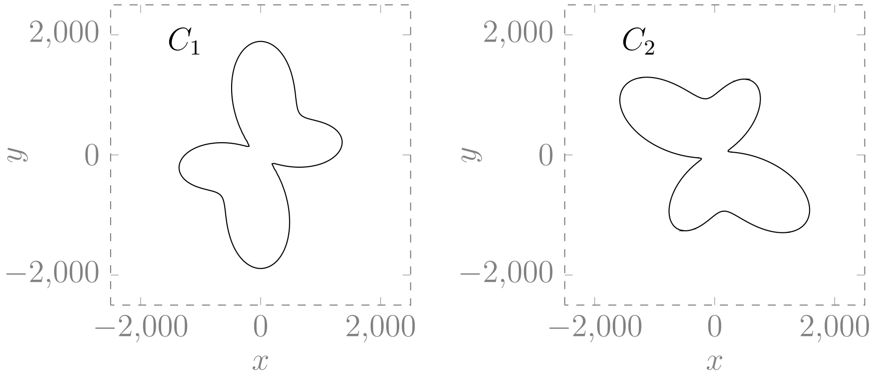

FIGURE 1.1. The curves C_1 and C_2 only differ by a rotation.

Regarding this question, we should be aware that each curve has *two* defining polynomials: If $f\colon S^1 \to \mathbb{R}$ describes $C \subset \mathbb{R}^2$, then its negative $-f$ describes the same set $C \subset \mathbb{R}^2$. With the intuition of describing the curve by deforming the unit circle, this ambiguity corresponds to turning the closed curve C inside out. With this in mind, we typically want to think of the curves defined by f and by $-f$ as two distinct objects (even though they are equal as subsets of $\mathbb{R}^2$). For example, the curve defined by the constant function $f \equiv 1$ is the unit circle, while the curve defined by $f \equiv -1$ should be considered as the unit circle turned inside out.

With this comment, it makes now sense to speak of "the" defining polynomial for a curve. Then the question from above corresponds to the following algebraic question:

Question 1.1. *Given two polynomials $f = \sum_{i=0}^{2d} a_i x^{2d-i} y^i$ and $g = \sum_{i=0}^{2d} b_i x^{2d-i} y^i$, how can we decide in terms of their coefficients a_i and b_i whether or not there exists an orthogonal transformation $\varphi\colon \mathbb{R}^2 \to \mathbb{R}^2$ such that $f = g \circ \varphi$ as functions $\mathbb{R}^2 \to \mathbb{R}$?*

Once we can decide whether two polynomials define equally shaped curves, a natural question is how to uniquely encode the shape of a curve, i.e. an equivalence class of curves up to orthogonal transformations. The corresponding question for polynomials is:

Question 1.2. *How can we encode in a unique way equivalence classes of polynomials up to orthogonal transformations?*

In the following Section, we will describe the mathematical setup for addressing Questions 1.1 and 1.2.

Note that we can formulate the entire setup for surfaces instead of curves by considering functions $f\colon S^2 \to \mathbb{R}$ on the unit sphere $S^2 \subset \mathbb{R}^3$, given by a polynomial expression

$$f(x,y,z) = \sum_{i+j+k=2d} a_{i,j,k} x^i y^j z^k$$

in three variables instead of only two, and by considering orthogonal transformations of the three-dimensional space $\mathbb{R}^3$. Similarly, we can generalize this to arbitrary higher dimensions, but in this thesis we will restrict the treatment to the geometrically most important cases of curves and surfaces.

1.2. Application in Neuroimaging

A specific application motivating the investigation in this Thesis comes from the active field of Neuroimaging. We may briefly summarize the background for this application as follows: In Neuroimaging, we are interested in understanding the structure of the brain by measuring electromagnetic responses of water molecules in the human brain under the influence of external electromagnetic fields and gradients. Specifically, techniques from Diffusion Magnetic Resonance Imaging (dMRI) extract information about directional restrictions of the random heat motion of water molecules – and these directional restrictions correlate to the the geometry of neuron fibers in the brain.

Roughly speaking, the brain is being discretized into small volume blocks (“voxels”) and for each of these volume blocks the measurements produce a (discretized) function $f\colon S^2 \to \mathbb{R}_{\geq 0}$ on the unit sphere $S^2 := \{v \in \mathbb{R}^3 \colon \|v\| = 1\}$, such that the value $e^{-f(v)} \in [0,1]$ for $v \in S^2$ describes the obstruction of the random heat motion in the direction v.[1] Typically, it is assumed that the diffusion obstruction in the directions v and $-v$ is equal, meaning that f is an even function on the sphere.

The diffusivity function f can therefore be approximated with homogeneous polynomials of even degree. In the simplest model, the function f may be assumed to be a homogeneous quadratic polynomial

$$f(x,y,z) = a_{200}x^2 + a_{020}y^2 + a_{002}z^2 + a_{110}xy + a_{101}xz + a_{011}yz.$$

In more advanced models, f is approximated by a homogeneous polynomal of degree $2d \geq 4$.

With the aim of understanding the local structure of the brain at a given voxel, we want to extract more reasonable information than just the coefficients a_{ijk} of the polynomial function $f = \sum a_{ijk} x^i y^j z^k$. We are interested in characteristics of the function f which are independent of the specific orientation in the brain.

[1] Here, a value of 1 for $e^{-f(v)}$ means no obstruction at all, and a value of 0 would mean total obstruction.

This corresponds to the task of computing invariants of homogeneous polynomial functions of even degree up to orthogonal transformations.

CHAPTER 2

Invariant Theory and algorithmic challenges

2.1. Notations

In order to make the following treatment mathematically precise, we start out with a few notational conventions. We assume some basic familiarity with algebraic language (group actions, rings, fields etc).

Throughout we will fix $n \geq 2$. We denote by $\mathbb{R}[x_1, \ldots, x_n]$ the set of polynomials

$$f = \sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n} x_1^{i_1} \cdot \ldots \cdot x_n^{i_n}$$

in the n variables $x_1, \ldots, x_n$ with real coefficients (i.e. $a_{i_1,\ldots,i_n} \in \mathbb{R}$). In the above notation, the sum ranges over all n-tuples $(i_1, \ldots, i_n)$ of non-negative integers and it is understood that only finitely many coefficients $a_{i_1,\ldots,i_n}$ are non-zero, so that the sum is finite.

We will focus on the cases $n = 2$ and $n = 3$ (and we introduce the notation for arbitrary n mainly in order to unify the treatment of those two cases). For these cases, we will without further notice replace the variables x_1 and x_2 (and x_3) by x and y (and z) wherever notationally more convenient.

For a polynomial f as above, the expressions $x_1^{i_1} \cdot \ldots \cdot x_n^{i_n}$ such that $a_{i_1,\ldots,i_n} \neq 0$ are called the *monomials* of f and its *degree* is defined to be $i_1 + \ldots + i_n$. The *degree* of a non-zero polynomial is defined to be the maximum among the degrees of all its monomials. We will focus on *homogeneous polynomials*, i.e. the case where all monomials have the same degree. Homogeneous polynomials in two resp. three variables are also called *binary forms* resp. *ternary forms*.

We denote by $\mathbb{R}[x_1, \ldots, x_n]_{2d}$ the set of homogeneous polynomials of degree $2d$.[1] A simple counting argument shows that there are $N := \binom{n-1+2d}{2d}$ monomials of degree $2d$, so we may identify a polynomial $f = \sum_{i_1 \ldots i_n} a_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n}$ with the N-tuple consisting of the coefficients $a_{i_1 \ldots i_n}$ for $i_1 + \ldots + i_n = 2d$ (for any fixed convention on how to order the entries of this N-tuple). Formally, $\mathbb{R}[x_1, \ldots, x_n]_{2d}$ is an N-dimensional vector space over $\mathbb{R}$ and identifying a polynomial with the tuple of its

[1] By convention, the zero-polynomial (i.e. where all $a_{i_1 \ldots i_n} = 0$) is also a homogeneous polynomial of degree $2d$ (for any d).

coefficients corresponds to an explicit isomorphism between the vector spaces $\mathbb{R}[x_1, \ldots, x_n]_{2d}$ and $\mathbb{R}^N$. In order to stress this point of view, we denote

$$V_{2d} := \mathbb{R}[x_1, \ldots, x_n]_{2d}$$

and, accordingly, we will from now on typically denote elements of V_{2d} by letters like v or w to stress that we view them as elements in a vector space (and may think of them simply as N-tuples).

By $O(n) \subset \mathbb{R}^{n \times n}$ we denote the group of orthogonal matrices, i.e. matrices $g \in \mathbb{R}^{n \times n}$ such that $g^T g = \mathrm{id}$. We consider the linear group action of $O(n)$ on the vector space V_{2d} given by

$$O(n) \times V_{2d} \to V_{2d}, \quad (g, v) \mapsto gv := v \circ g^{-1}.$$

Here, by $v \circ g^{-1}$, we mean the composition of the orthogonal transformation $g^{-1} \colon \mathbb{R}^n \to \mathbb{R}^n$ with the polynomial function $v \colon \mathbb{R}^n \to \mathbb{R}$, resulting in a different polynomial function which we denote by gv (and which is still homogeneous of degree $2d$). The use of the inverse g^{-1} instead of g in the above composition is only of notational importance, guaranteeing $g_1(g_2 v) = (g_1 g_2)v$. It is worth noting that $g^{-1} = g^T$ for any $g \in O(n)$ by definition.

We say that $v \in V_{2d}$ and $w \in V_{2d}$ are *orthogonally equivalent* if there exists an orthogonal transformation $g \in O(n)$ such that $w = gv$.

On a formal level, this group action is given as follows: Let $g = (g_{ij}) \in O(n)$ be an orthogonal $n \times n$-matrix with entries g_{ij} and let $v = \sum_{i_1 \ldots i_n} a_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n} \in V_{2d}$. Applying the substitutions

$$x_k \mapsto g_{1k} x_1 + g_{2k} x_2 + \ldots + g_{nk} x_n$$

to the homogeneous polynomial v and expanding the resulting expression gives the new homogeneous polynomial $gv \in V_{2d}$.

Example 2.1. For $n = 2$ and $d = 4$ let $g = \begin{pmatrix} 3/5 & -4/5 \\ 4/5 & 3/5 \end{pmatrix} \in O(2)$ and $v = x^4 + 3x^3y + 2x^2y^2 \in V_4$. Then

$$\begin{aligned} gv &= \left(\frac{3}{5}x + \frac{4}{5}y\right)^4 + 3\left(\frac{3}{5}x + \frac{4}{5}y\right)^3 \cdot \left(-\frac{4}{5}x + \frac{3}{5}y\right) \\ &\qquad + 2\left(\frac{3}{5}x + \frac{4}{5}y\right)^2 \cdot \left(-\frac{4}{5}x + \frac{3}{5}y\right)^2 \\ &= \frac{9}{125}x^4 - \frac{57}{125}x^3y - \frac{1018}{625}x^2y^2 + \frac{192}{125}xy^3 + \frac{224}{125}y^4. \end{aligned}$$

Analogously, we can check the example from Figure 1.1 as claimed in Section 1.1.

From the definition of the group action of $O(n)$ on V_{2d} (with the viewpoint of composing functions, or with the formal viewpoint of variable substitutions), it is immediate that $g(v + w) = gv + gw$ and

$g(\lambda \cdot v) = \lambda \cdot gv$ holds for all $g \in O(n)$, $v, w \in V_{2d}$ and $\lambda \in \mathbb{R}$, i.e. the action of $O(n)$ on V_{2d} is a *linear group action.*

2.2. The Invariant Theory approach

With the notations established in Section 2.1, Question 1.1 can be reformulated as follows:

Question 2.2. *Given $v, w \in V_{2d}$, does there exist $g \in O(n)$ such that $w = gv$?*

Invariant Theory provides a general setup for studying such questions. We start out with an example motivating the further approach.

Example 2.3. We consider $n = 2$ and $2d = 2$, i.e. the case of *binary quadratic forms*: Let $v = ax^2 + bxy + cy^2 \in V_2$. Any 2×2 rotation matrix is given as $g = \begin{pmatrix} s & -t \\ t & s \end{pmatrix}$, where $s^2 + t^2 = 1$. Then

$$\begin{aligned} gv &= a(sx+ty)^2 + b(sx+ty)(-tx+sy) + c(-tx+sy)^2 \\ &= \tilde{a}x^2 + \tilde{b}xy + \tilde{c}y^2, \end{aligned}$$

where

$$\tilde{a} = as^2 - bst + ct^2,\ \tilde{b} = 2ast + bs^2 - bt^2 - 2cst,\ \tilde{c} = at^2 + bst + cs^2.$$

Regarding Question 2.2, we conclude that another $w = \hat{a}x^2 + \hat{b}xy + \hat{c}y^2 \in V_2$ only differs from v by an orthogonal transformation if the following system of four equations in two variables s, t has a real solution:

$$\begin{aligned} as^2 - bst + ct^2 &= \hat{a}, \\ 2ast + bs^2 - bt^2 - 2cst &= \hat{b}, \\ at^2 + bst + cs^2 &= \hat{c}, \\ s^2 + t^2 &= 1. \end{aligned}$$

Note that this is a non-linear system of equations. In this particular case ($n = 2d = 2$) determining whether such a system of equations has a real solution is feasible, but for higher values of d or n, the number of equations and variables as well as the degree of the equations increase and with these, the complexity of solving the system of equations quickly becomes infeasible.

Instead, we take a different approach: Note that

$$\tilde{a} + \tilde{c} = (as^2 - bst + ct^2) + (at^2 + bst + cs^2) = a + c$$

(using $s^2 + t^2 = 1$) and similarly, one can check

$$\begin{aligned}\tilde{a}^2 + \frac{1}{2}\tilde{b}^2 + \tilde{c}^2 = (as^2 - bst + ct^2)^2 + \frac{1}{2}(2ast + bs^2 - bt^2 - 2cst)^2 \\ + (at^2 + bst + cs^2)^2 \\ = (a^2 + \frac{1}{2}b^2 + c^2)(s^2 + t^2)^2 = a^2 + \frac{1}{2}b^2 + c^2.\end{aligned}$$

Hence, if we are interested in comparing $v = ax^2 + bxy + cy^2$ and $w = \hat{a}x^2 + \hat{b}xy + \hat{c}y^2$, we conclude: *If $a + b \neq \hat{a} + \hat{b}$ or $a^2 + \frac{1}{2}b^2 + c^2 \neq \hat{a}^2 + \frac{1}{2}\hat{b}^2 + \hat{c}^2$, then there does not exist any $g \in O(n)$ such that $w = gv$.*

In fact, we will see later in Theorem 3.13 that the converse is also true in this case, i.e. if $a + b = \hat{a} + \hat{b}$ and $a^2 + \frac{1}{2}b^2 + c^2 = \hat{a}^2 + \frac{1}{2}\hat{b}^2 + \hat{c}^2$, then v and w only differ by an orthogonal transformation. Therefore, instead of solving a non-linear system of equations as above, we can simply calculate the two values $a + b$ and $a^2 + \frac{1}{2}b^2 + c^2$ to answer Question 2.2. This also gives an answer to Question 1.2: Elements of V_2 can be encoded up to orthogonal transformations by only storing their values $a + b$ and $a^2 + \frac{1}{2}b^2 + c^2$.

Motivated by this example, our approach is to find polynomial expressions (like $a^2 + \frac{1}{2}b^2 + c^2$ from above) – or, more generally, rational expressions – which remain unchanged under the action by any orthogonal transformation. To make this formal, we define:

Definition 2.4. We denote by $\mathcal{O}(V_{2d})$ the set of polynomial functions $P\colon V_{2d} \to \mathbb{R}$. Explicitly, if we denote elements of V_{2d} as

$$\sum_{i_1+\ldots+i_n=2d} a_{i_1\ldots i_n} x_1^{i_1} \ldots x_n^{i_n}$$

(and in this way identify them with N-tuples $(a_{i_1\ldots i_n}) \in \mathbb{R}^N$), then $\mathcal{O}(V_{2d})$ is the set of polynomial expressions in the variables $a_{i_1\ldots i_n}$. We then define the set of **polynomial invariants** as

$$\mathcal{O}(V_{2d})^{O(n)} := \{P \in \mathcal{O}(V_{2d}) \mid P(v) = P(gv)\ \forall v \in V_{2d}, g \in O(n)\}.$$

Note that the fact that we consider the space V_{2d} does *not* mean that the degree of a polynomial invariant $P \in \mathcal{O}(V_{2d})^{O(n)}$ (as polynomial expression in the variables $a_{i_1\ldots i_n}$) is bounded by $2d$. In fact, $\mathcal{O}(V_{2d})^{O(n)}$ contains polynomial invariants of arbitrarily high degree in general.

Example 2.5. Coming back to the Example 2.3, we denoted elements of V_2 as $ax^2 + bxy + cy^2$, so we may consider them as points (a, b, c) in $\mathbb{R}^3$. With this notation, $\mathcal{O}(V_2)$ is the set of polynomials in the variables a, b and c, i.e. $\mathcal{O}(V_2) = \mathbb{R}[a, b, c]$. We have seen in Example 2.3 that

$$a + c \in \mathcal{O}(V_2)^{O(2)} \quad \text{and} \quad a^2 + \frac{1}{2}b^2 + c^2 \in \mathcal{O}(V_2)^{O(2)}.$$

How many polynomial invariants are there? Of course, the answer is in general: infinitely many. The reason is that adding or multiplying any two polynomial invariants as well as multiplying a polynomial invariant with a real number results again in a polynomial invariant. (In algebraic language, $\mathcal{O}(V_{2d})^{O(n)}$ is an $\mathbb{R}$-*algebra.*) However, the following deep theorem states that up to this observation, there are only finitely many invariants.

Theorem 2.6. *For any d and n there exists a* finite set $\{p_1, \dots, p_m\} \subset \mathcal{O}(V_{2d})^{O(n)}$ *of polynomial invariants which generate $\mathcal{O}(V_{2d})^{O(n)}$ as $\mathbb{R}$-algebra. This means that any other polynomial invariant $q \in \mathcal{O}(V_{2d})^{O(n)}$ can be written as*

$$q = \sum_{i_1,\dots,i_m} \mu_{i_1,\dots,i_m} p_1^{i_1} \cdot \dots \cdot p_m^{i_m},$$

i.e. as a polynomial expression in terms of $p_1, \dots, p_m$. We call such a finite set $\{p_1, \dots, p_m\}$ a set of ***generating polynomial invariants****.*

This is a fundamental result which can be traced back to Hilbert and we refer to [**DK02**, Theorem 2.2.10] for one of many textbook references. In fact, this theorem is not specific to our context, but holds more generally for any linear action of a group G (in our case $O(n)$) on a finite-dimensional vector space (in our case V_{2d}), as long as G is a *reductive algebraic group* (which is the case for $O(n)$, see e.g. [**GW09**, Theorem 3.3.11]). Theorem 2.6 is a very important result and forms the basis of Invariant Theory. It is important to note that the finite set $\{p_1, \dots, p_m\}$ is not unique. Furthermore, the proof of this Theorem only establishes the existence of such $p_1, \dots, p_m$ in a *non-constructive* way, leaving the question how to determine such generating polynomial invariants as an algorithmic challenge.

Example 2.7. In Example 2.3, we saw that $p_1 := a + c$ and $p_2 := a^2 + \frac{1}{2}b^2 + c^2$ are polynomial invariants in the case of V_2. It can equally be checked that $q := 4ac - b^2$ is a polynomial invariant. However, this is not a "new" invariant, as it can be written as: $q = 2p_1^2 - 2p_2$. In fact, we will see later in Theorem 3.13 and Remark 3.16 that p_1 and p_2 are generating polynomial invariants as stated in Theorem 2.6. An alternative choice for generating polynomial invariants would be p_1 and q.

Another important fact is the following theorem:

Theorem 2.8. *Let $p_1, \dots, p_m \in \mathcal{O}(V_{2d})^{O(n)}$ be generating polynomial invariants. Then $v, w \in V_{2d}$ are orthogonally equivalent (i.e. there exists $g \in O(n)$ such that $w = gv$) if and only if $p_i(v) = p_i(w)$ holds for all $i \in \{1, \dots, m\}$.*

For a proof, we refer to [**Oli14**, Proposition 2.3.31]. In general, this theorem holds for a linear action of any *compact* group on an $\mathbb{R}$-vector space.

Theorem 2.8 gives a crucial justification for approaching Question 1.1 by methods of polynomial invariants. It further addresses Question 1.2 of how to encode polynomials up to orthogonal transformations: We may encode $v \in V_{2d}$ as the m-tuple $(p_1(v), \dots, p_m(v))$. Then the m-tuples of $v \in V_{2d}$ and $w \in V_{2d}$ are equal if and only if v and w are orthogonally equivalent.

This raises some further questions, for example: *Is a given m-tuple $(\mu_1, \dots, \mu_m) \in \mathbb{R}^m$ such an encoding of a polynomial $v \in V_{2d}$? And if so, can we reconstruct one v (unique only up to orthogonal transformations) such that $p_i(v) = \mu_i$?* We call this the *Reconstuction Problem.*

In any case, the first crucial question is: How do we find a set of generating polynomial invariants? General algorithms for determining a set of generating polynomial invariants (for the action of any reductive algebraic group on a vector space) based on Gröbner basis algorithms exist (see for example [**DK02**, Section 4.1]), but their complexity increases drastically with the dimension of V_{2d}, which in turn grows quickly with d – recall $\dim V_{2d} = \binom{n-1+2d}{2d}$. Already for $n = 3$ and $2d = 4$, these general methods are very far from a feasible computation.

Instead, it is necessary to exploit mathematically the setting of the specific action of $O(n)$ on V_{2d}. In [**AKO16**], a set of generating polynomial invariants for $n = 3$, $2d = 4$ has been determined. However, the number of these generating polynomial invariants is $m = 64$, while $\dim V_4 = 15$. This means that with the above approach to Question 1.2, we would encode elements of V_4 (which we can think of as 15-tuples of coefficients) up to orthogonal transformations as a 64-tuple. In [**AKO16**], it has further been shown in that 64 is in fact the minimal number of generating polynomial invariants.

With increasing degree $2d$, the number of generating polynomial invariants grows very large and determining them becomes more and more difficult. Furthermore, it is unclear how to feasibly approach the reconstruction problem mentioned above as well as similar algorithmic questions for a high number of invariants like 64.

For this reason, in the following section we will slightly relax the approach motivated here, in order to obtain results that are more compact.

2.3. From polynomial invariants to rational invariants

We now extend the viewpoint from invariants which are polynomial expressions to invariants which are rational expressions, i.e. fractions of two polynomial expressions. We start out fixing a notation analogous to Definition 2.4.

Definition 2.9. We denote by $K(V_{2d})$ the set of rational functions $p\colon V_{2d} \dashrightarrow \mathbb{R}$. Explicitly, if we denote elements of V_{2d} as

$$\sum_{i_1+\ldots+i_n=2d} a_{i_1\ldots i_n} x_1^{i_1} \ldots x_n^{i_n},$$

then $K(V_{2d})$ is the set of rational expressions (i.e. a fraction of polynomial expressions) in the variables $a_{i_1\ldots i_n}$. In the same way as before, we then define the set of **rational invariants** as

$$K(V_{2d})^{O(n)} := \{p \in K(V_{2d}) \mid p(v) = p(gv)\ \forall v \in V_{2d}, g \in O(n)\ ^2\}.$$

Remark 2.10. When working with rational expressions $p = \frac{p_1}{p_0} \in K(V_{2d})$ (where p_1 and $p_2 \neq 0$ are polynomial expressions), there is always an issue of division by zero. In particular, note that $p = \frac{p_1}{p_0}$ defines a function only on the set $\{v \in V_{2d} \mid p_0(v) \neq 0\}$ and the value $p(v)$ is undefined whenever $p_0(v) = 0$. We say that the function p is only *defined on a general point*, and to keep this in mind, the function is typically denoted by a dashed arrow $p\colon V_{2d} \dashrightarrow \mathbb{R}$. We follow that convention.

In general, when working with rational functions, the following definition is a useful notational convention:

Convention 2.11. Let $\mathcal{P}$ be a statement about points $v \in V$ in a given $\mathbb{R}$-vector space V (e.g. $V = V_{2d}$). We say that $\mathcal{P}$ holds for a **general point** if there exists a non-zero[3] polynomial function $p_0\colon V \to \mathbb{R}$ such that $\mathcal{P}$ holds for all points $v \in V$ where $p_0(v) \neq 0$.

The idea behind this convention is that the vanishing set $\{v \in V \mid p_0(v) = 0\}$ of a polynomial p_0 can be thought of as a very small, neglectable subset of the vector space V. Of course, the above is not a very precise and formal definition, since we leave vague what we mean by a "statement about points". Typically, this is a property which can be formulated by some logical expression or algebraic identity, but instead of trying to make this precise, we leave the above convention in its informal formulation. It should be always clear in the contexts where we use the term *general point* in this thesis.

[2] wherever $p(v)$ and $p(gv)$ are defined, i.e. where the denominator is non-zero

[3] Recall that a *non-zero polynomial* is a polynomial function which is not everywhere zero, but it typically still has points where it takes the value 0.

Observation 2.12. *Let $p, q\colon V_{2d} \to \mathbb{R}$ be polynomial functions. If $p(v) = q(v)$ holds for a general point $v \in V$, then the polynomials p and q already agree everywhere. This follows from continuity of the polynomial functions p and q. A similar observation holds for rational functions.*

While with polynomial invariants we could speak about scalar multiplication as well as multiplying and adding two polynomial invariants, for rational invariants we can now also speak about dividing two rational functions by each other. (In algebraic language, $K(V_{2d})^{O(n)}$ is a *field extension* of $\mathbb{R}$.) The following finiteness result is therefore the analogue to Theorem 2.6 for rational invariants.

Theorem 2.13. *For any d and n there exists a* finite set $\{p_1, \dots, p_m\} \subset K(V_{2d})^{O(n)}$ *of rational invariants which generate $K(V_{2d})^{O(n)}$ as a field extension of $\mathbb{R}$. This means that any other rational invariant $q \in K(V_{2d})^{O(n)}$ can be written as a rational expression in terms of $p_1, \dots, p_m$. We call such a finite set $\{p_1, \dots, p_m\}$ a set of **generating rational invariants**.*

In contrast to Theorem 2.6 this is not a very deep theorem, but follows from basic facts in Field Theory (see for example [**Isa09**, Theorem 24.9]). The analogue to Theorem 2.8 is the following result from [**VP94**, Lemma 2.1, Theorem 2.3]:

Theorem 2.14. *Rational invariants $p_1, \dots, p_m \in K(V_{2d})^{O(n)}$ form a set of generating rational invariants if and only if for general points $v, w \in V_{2d}$ the following holds:*

$$w = gv \textit{ for some } g \in O(n) \;\Leftrightarrow\; p_i(v) = p_i(w)\ \forall i \in \{1, \dots, m\}.$$

Note that Theorem 2.14 is more than just an analogue of Theorem 2.8, as it additionally contains a reverse implication. This is a difference between polynomial and rational invariants: It is in general *not* true that the property

$$w = gv \text{ for some } g \in O(n) \;\Leftrightarrow\; p_i(v) = p_i(w)\ \forall i \in \{1, \dots, m\}$$

would imply that polynomial invariants $p_1, \dots, p_m$ form a set of generating polynomial invariants.

Considering rational invariants instead of polynomial invariants will greatly decrease the minimal number of generating invariants needed. In fact, the main result of this thesis will be the construction of a set of $\dim V_{2d} - \dim O(n) = \binom{n-1+2d}{2d} - \binom{n}{2}$ generating rational invariants for $n = 2, 3$. For example, for V_4 this means 12 generating rational invariants instead of 64 generating polynomial invariants. In fact, this is the minimal cardinality of a set of generating rational invariants by the following result, following from [**VP94**, Corollary of Theorem 2.3]:

Theorem 2.15. *For $n, d \geq 2$ any set of generating rational invariants for the action of $O(n)$ on V_{2d} consists of at least* $\dim V_{2d} - \dim O(n) = \binom{n-1+d}{d} - \binom{n}{2}$ *elements.*

2.4. Algorithmic challenges

From the above discussions, the following algorithmic challenges arise:

1. Compute a set of generating rational invariants $p_1, \ldots, p_m \in K(V_{2d})^{O(n)}$.
2. **Evaluation Problem**: Evaluate $p_1(v), \ldots, p_m(v)$ for a given point $v \in V_{2d}$ in an efficient and robust way.
3. **Reconstruction Problem**: Which m-tuples $\mu = (\mu_1, \ldots, \mu_m) \in \mathbb{R}^m$ lie in the image of the map
$$\pi \colon V_{2d} \dashrightarrow \mathbb{R}^m, \quad v \mapsto (p_1(v), \ldots, p_m(v))?$$
If μ lies in the image of π, find a representative $v \in V_{2d}$ such that $\pi(v) = \mu$.
4. **Rewriting Problem**: Given a rational invariant $q \in K(V_{2d})^{O(n)}$, rewrite q as a rational expression in terms of $p_1, \ldots, p_m$.

We will of course start out with the first algorithmic challenge. How to address the remaining challenges will become more apparent from our construction of the generating rational invariants.

CHAPTER 3

Main technique: The slice method

Our aim is to determine generating rational invariants for the linear action of the orthogonal group $O(n)$ on the vector space V_{2d}. The group $O(n)$ is infinite, in fact it is of dimension $\dim O(n) = \binom{n}{2}$ as an algebraic group. We reduce the problem to the simpler question of determining rational invariants for the linear action of a *finite* group B_n (contained in $O(n)$ as a subgroup) on a smaller vector space Λ (contained in V_{2d}).

In Section 3.1, we introduce the general technique for this reduction, called the *slice method*. Then, we illustrate this method in Section 3.2 for V_2, i.e. we determine generating rational invariants for the case of homogeneous quadratic polynomials (also called *quadratic forms*). This quadratic case will also serve as motivation and as a starting point for the treatment of the general case of V_{2d}. We will finish this chapter by specifying a *slice* for V_{2d} in Section 3.3.

3.1. The Slice Lemma

In order to formulate the main technique, we need to slightly abstract from our setting: We consider a linear action of an algebraic group G on a finite-dimensional $\mathbb{R}$-vector space V, denoted

$$G \times V \to V, \quad (g, v) \mapsto gv.$$

In our case, we have $G = O(n)$ and $V = V_{2d}$, and the action is given as defined in Section 2.1. We define $K(V)$ and $K(V)^G$ completely analogous to Definition 2.9 and call elements of $K(V)^G$ *rational invariants* for the action of G on V. Theorems 2.13 and 2.14 generalize to $K(V)^G$ in the straightforward way.

We introduce this more general notion, because we reduce the study of rational invariants $K(V_{2d})^{O(n)}$ to the study of rational invariants $K(\Lambda_{2d})^{B_n}$ for a simpler action of a *finite* group $B_n \subset O(n)$ on a smaller vector space $\Lambda_{2d} \subset V_{2d}$.

The main technique is a theorem known as the *Slice Lemma*. It is based on the following definition (recall Convention 2.11).

Definition 3.1. Consider a linear group action of an algebraic group G on a finite-dimensional $\mathbb{R}$-vector space V. A subspace $\Lambda \subset V$ is called a **slice** for the group action, and the subgroup

$$B := \{g \in G \mid gs \in \Lambda \ \forall s \in \Lambda\} \subset G$$

is called its **stabilizer**, if the following two properties hold:

(i) For a general point $v \in V$ there exists $g \in G$ such that $gv \in \Lambda$.
(ii) For a general point $s \in \Lambda$ the following holds: If $g \in G$ is such that $gs \in \Lambda$, then $g \in B$.

The Slice Lemma then states that rational invariants of the action of G on V are in one-to-one correspondence with rational invariants of the smaller group $B \subset G$ on the slice $\Lambda \subset V$:

Theorem 3.2 (Slice Lemma)**.** *Let Λ be a slice of a linear action of an algebraic group G on a finite-dimensional $\mathbb{R}$-vector space V, and let B be its stabilizer. Then there is a one-to-one correspondence*[1] *between rational invariants*

$$\varrho\colon K(V)^G \overset{\cong}{\to} K(\Lambda)^B, \ p \mapsto p|_\Lambda$$

which restricts a rational invariant $p\colon V \dashrightarrow \mathbb{R}$ to $p|_\Lambda\colon \Lambda \dashrightarrow \mathbb{R}$.

We will apply this theorem for $G = O(n)$, $V = V_{2d}$ and a suitable choice for the slice Λ. Since this theorem is at the heart of our construction of generating rational invariants, we will give the most relevant ideas of the argument. For a complete proof with full details, we refer to [**CTS07**, Theorem 3.1].

Proof (Outline). First, it has to be checked that restricting a rational invariant $p = \frac{p_1}{p_0} \in K(V)^G$ to Λ gives a rational invariant for the action of B on Λ. It is not hard to show that property (i) of Definition 3.1 implies that p_0 does not simultaneously vanish at all points $s \in \Lambda$, so $p|_\Lambda$ is in fact a well-defined rational function. To show that $p|_\Lambda$ is a rational invariant, consider $g \in B \subset G$ and $s \in \Lambda \subset V$. Then $gs \in \Lambda$ and $p|_\Lambda(gs) = p(gs) = p(s)$, because p is a rational invariant (for the action of G on V).

From the definition it is immediate that this map $\varrho\colon K(V)^G \to K(\Lambda)^B$ is a field homomorphism over $\mathbb{R}$, i.e. it is compatible with addition and multiplication of invariants, and constant invariants correspond to the same constant invariants. It is a general fact that being a field homomorphism implies injectivity (see e.g. [**AM69**, Proposition 1.2]), hence we deduce that $p|_\Lambda = \tilde{p}|_\Lambda$ for $p, \tilde{p} \in K(V)^G$ already implies $p = \tilde{p}$.

[1] More exactly, ϱ is a *field isomorphism over* $\mathbb{R}$, i.e. this one-to-one correspondence satisfies: $\varrho(p + \tilde{p}) = \varrho(p) + \varrho(\tilde{p})$, $\varrho(p \cdot \tilde{p}) = \varrho(p) \cdot \varrho(\tilde{p})$ and $\varrho(\lambda) = \lambda$ for all constant rational functions given by a scalar $\lambda \in \mathbb{R}$.

It remains to show that ϱ is surjective, i.e. that given a rational invariant $q\colon \Lambda \dashrightarrow \mathbb{R}$ for the action of B on Λ, there must exist a rational invariant $p\colon V \dashrightarrow \mathbb{R}$ such that $p|_\Lambda = q$. To show this, we have to define the value $p(v)$ for a general point $v \in V$. This is done as follows: Let $g \in G$ be a such that $gv \in \Lambda$ – such g exists for general v by property (i) of Definition 3.1. For a sufficiently general point $v \in V$ we can also assume that $q\colon \Lambda \dashrightarrow \mathbb{R}$ is defined at the point $g_0 v \in \Lambda$. Then we define $p(v) := q(g_0 v)$.

For a general point v, this definition does not depend on the choice of $g_0 \in G$ such that $g_0 v \in \Lambda$. Indeed, if $g_0' \in G$ is a different choice such that $g_0' v \in \Lambda$, then $g_0' g_0^{-1} \in G$ maps $g_0 v \in \Lambda$ to $g_0' v \in \Lambda$, so by property (ii) of Definition 3.1, we have $g_0' g_0^{-1} \in B$ (if $v \in V$ is a sufficiently general point). Therefore, $q(g_0' v) = q((g_0' g_0^{-1})(g_0 v)) = q(g_0 v)$, since $q \in K(\Lambda)^B$ is a rational invariant for the action of B on Λ. Hence, the above construction defines a map $p\colon V \dashrightarrow \mathbb{R}$. It can be shown that this p is in fact given by a rational expression.

Finally, we have to check that this constructed $p\colon V \dashrightarrow \mathbb{R}$ lies in $K(V)^G$, i.e. $p(v) = p(gv)$ for any $g \in G$ and a general point $v \in V$. For that, note that $g_0 g^{-1}$ is an element of G such that $(g_0 g^{-1})(gv) \in \Lambda$. Hence, the value $p(gv)$ is defined as $q((g_0 g^{-1})(gv)) = q(g_0 v)$, which is $p(v)$ by construction. □

Remark 3.3. We included the idea of the proof in order to provide insight to the main technique exploited in our approach. Worth remembering from the proof is that the inverse to the map

$$\varrho\colon K(V)^G \xrightarrow{\cong} K(\Lambda)^B,\ p \mapsto p|_\Lambda$$

is given by

$$\begin{aligned} &\varrho^{-1}\colon K(\Lambda)^B \to K(V)^B, \\ &\qquad q \mapsto \Big(V \dashrightarrow \mathbb{R},\ v \mapsto q(gv),\ \text{where } g \in G \text{ such that } gv \in \Lambda\Big). \end{aligned}$$

For the construction of *generating* rational invariants we deduce from Theorem 3.2 the following:

Corollary 3.4. *Let Λ be a slice of a linear action of an algebraic group G on a finite-dimensional $\mathbb{R}$-vector space V, and let B be its stabilizer. If $\{p_1, \dots, p_m\}$ is a set of generating rational invariants for the action of B on Λ, then $\{\varrho^{-1}(p_1), \dots, \varrho^{-1}(p_m)\}$ is a set of generating rational invariants for the action of G on V (where ϱ is given as above).*

Proof. This is a formal consequence of the fact that $\varrho\colon K(V)^G \xrightarrow{\cong} K(\Lambda)^B$ is a field isomorphism. Indeed, if $q \in K(V)^G$, then $\varrho(q)$ can by assumption be written as a rational expression in the generators $p_1, \dots, p_m$. Then the fact that ϱ^{-1} is compatible with addition and multiplication implies that $q = \varrho^{-1}(\varrho(q))$ is the same rational expression in $\varrho^{-1}(p_1), \dots, \varrho^{-1}(p_m)$. □

Remark 3.5. It should be noted that this result does not hold for polynomial invariants (or at least a corresponding statement for polynomial invariants requires stronger hypotheses on the slice). In particular, even if $p_1, \dots, p_m \in K(\Lambda)^B$ are *polynomial* expressions, the construction described above typically introduces denominators, so that $\varrho^{-1}(p_1), \dots, \varrho^{-1}(p_m) \in K(V)^G$ are *rational* expressions.

3.2. Invariants for quadratic forms

In this section, we apply the method from Section 3.1 to the case for $d = 1$, i.e. we study rational invariants for the action of $O(n)$ on V_2. None of the results in this section are new, but we give a presentation of these facts which illustrates the use of the Slice Method and which serves as a starting point for investigating the case $d \geq 2$.

Elements of V_2 are called *quadratic forms* and can be written in the form $v = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} x_i x_j \in V_2$, where $a_{ij} = a_{ji}$ for $i \neq j$. Note that in this notation the coefficient of $x_i x_j$ $(= x_j x_i)$ for $i \neq j$ is $a_{ij} + a_{ji} = 2a_{ij}$. This allows to write

$$v = x^T \cdot A \cdot x,$$

where we define the vector of variables $x := \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ and where $A = (a_{ij}) \in \mathbb{R}^{n \times n}$ is the symmetric $n \times n$-matrix with entries a_{ij}. We call A the **Gramian matrix** of $v \in V_2$. We may therefore consider V_2 as the set of symmetric $n \times n$-matrices.

Example 3.6. For $n = 3$ the quadratic form[2] $v = 3x^2 + 2xy + 8y^2 - 14yz \in V_2$ can be written as

$$v = \begin{pmatrix} x & y & z \end{pmatrix} \cdot \begin{pmatrix} 3 & 1 & 0 \\ 1 & 8 & -7 \\ 0 & -7 & 0 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

Hence, we identify v with its Gramian matrix $\begin{pmatrix} 3 & 1 & 0 \\ 1 & 8 & -7 \\ 0 & -7 & 0 \end{pmatrix}$.

The following observation shows how the action of $O(n)$ on V_2 is given in terms of Gramian matrices:

Proposition 3.7. *Let $g \in O(n) \subset \mathbb{R}^{n \times n}$ and let $v \in V_2$ with Gramian matrix $A \in \mathbb{R}^{n \times n}$. Then the Gramian matrix of $gv \in V_2$ is the matrix product gAg^T (which is equal to gAg^{-1}).*

[2] Recall that we replace the variables x_1, x_2, x_3 with x, y, z for a more convenient notation.

Proof. The quadratic form $v \in V_2$ is the function $v\colon \mathbb{R}^n \to \mathbb{R}$ given by

$$v(x) = x^T A x$$

(where $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{R}^n$). By definition, $gv \in V_2$ is the function $gv\colon \mathbb{R}^n \to \mathbb{R}$ mapping $x \in \mathbb{R}^n$ to $v(g^{-1}x)$. Hence,

$$(gv)(x) = v(g^{-1}x) = (g^{-1}x)^T A(g^{-1}x) = x^T g A g^T x,$$

where we used $g^{-1} = g^T$ in the last step (which holds because $g \in O(n)$). Hence, $gAg^T = gAg^{-1}$ is the Gramian matrix of the quadratic form gv. □

In particular, two quadratic forms associated to symmetric matrices $A, B \in \mathbb{R}^{n\times n}$ are orthogonally equivalent if and only if there exists an orthogonal matrix g such that $B = gAg^T$. In order to apply the Slice Lemma, we define the following subspace of V_2:

Definition 3.8. Let $\Lambda_2 \subset V_2$ denote the subspace of quadratic forms whose Gramian matrix is a diagonal matrix. Explicitly,

$$\Lambda_2 = \{\sum_{i=1} \lambda_i x_i^2 \in V_2 \mid \lambda_1, \ldots, \lambda_n \in \mathbb{R}\}.$$

We will henceforth denote by $\operatorname{diag}(\lambda_1, \ldots, \lambda_n)$ the diagonal $n\times n$-matrix with entries $\lambda_1, \ldots, \lambda_n \in \mathbb{R}^n$.

Then the following is essentially a reformulation the Spectral Theorem for symmetric matrices.

Proposition 3.9. *The subspace $\Lambda_2 \subset V_2$ is a slice for the action of $O(n)$ on V_2. Its stabilizer $B_n \subset O(n)$ is the subgroup of $O(n)$ of* signed permutation matrices, *i.e. matrices for which each row and each column contain only one non-zero entry and this entry is either 1 or -1.*

Proof. To check that Λ_2 satisfies property (i) of Definition 3.1, let $v \in V_2$ and let $A = (a_{ij}) \in \mathbb{R}^{n\times n}$ be its Gramian matrix. The Spectral Theorem for symmetric matrices states that the eigenvalues of A are real numbers, which we denote $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$, and that we can choose an orthonormal set of corresponding eigenvectors $u_1, \ldots, u_n \in \mathbb{R}^n$. Let $g \in \mathbb{R}^{n\times n}$ be the matrix whose i-th row is the vector u_i^T. Then $g \in O(n)$, since an $n \times n$-matrix is an element of $O(n)$ if and only if it has orthonormal rows. The fact that $Au_i = \lambda_i u_i$ for all $i \in \{1, \ldots, n\}$ can be written as

$$Ag^T = g^T \operatorname{diag}(\lambda_1, \ldots, \lambda_n),$$

in other words gAg^T is a diagonal matrix. By Proposition 3.7, this means $gv \in \Lambda_2$, confirming property (i) of Definition 3.1.[3]

[3] Note that here we checked the property for *all* $v \in V_2$ and did not need to restrict to a *general point*, as would be allowed by Definition 3.1.

If g is an element of the stabilizer $B_n := \{g \in O(n) \mid gs \in \Lambda_2 \ \forall s \in \Lambda_2\}$, then the matrix product $g\,\mathrm{diag}(\lambda_1, \ldots, \lambda_n)g^T$ is by Proposition 3.7 again a diagonal matrix for all values of $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$. In particular, this holds when $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$ are *distinct*. If $A := \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$, then the fact that gAg^T is a diagonal matrix implies that the rows of g are orthonormal eigenvectors of the matrix A (by reversing the argument from above). The only unit-length eigenvectors of A are $\pm e_i$ (here we use the fact that the eigenvalues $\lambda_1, \ldots, \lambda_n$ are distinct), where e_i is the i-th canonical basis vector. Hence, $g \in B_n$ is a signed permutation matrix. Conversely, it is immediately checked that for any signed permutation matrix g, the matrix product $g\,\mathrm{diag}(\lambda_1, \ldots, \lambda_n)g^T$ is always a diagonal matrix. This establishes the description of the stablizer B_n.

Finally, we show property (ii) of Definition 3.1. By Proposition 3.7, this property is: If $g \in O(n)$ is such that for a *general point* $(\lambda_1, \ldots, \lambda_n) \in \mathbb{R}^n$, the matrix product $g\,\mathrm{diag}(\lambda_1, \ldots, \lambda_n)g^T$ is again a diagonal matrix, then $g \in B_n$. Indeed, we have just seen that this property holds whenever $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$ are n distinct values. It therefore only remains to remark that a *general point* $(\lambda_1, \ldots, \lambda_n) \in \mathbb{R}^n$ has distinct entries, because this is the case for all points in $\mathbb{R}^n$ where the polynomial function $\mathbb{R}^n \to \mathbb{R}$ given by the polynomial expression $\prod_{i<j}(x_i - x_j)$ does not vanish. □

Then Theorem 3.2 implies

Corollary 3.10. *There is a one-to-one correspondence between rational invariants*

$$\rho\colon K(V_2)^{O(n)} \overset{\cong}{\to} K(\Lambda_2)^{B_n}$$

which is given by restriction of rational functions.

Above, we described the group $B_n \subset O(n)$ as the set of signed permutation matrices. Note that this group has $2^n \cdot n!$ elements. An alternative description is that B_n is the smallest group containing all *permutation matrices* and all *sign-change matrices* (i.e. diagonal matrices whose diagonal entries are ± 1). This follows from the following remark:

Remark 3.11. Each element $g \in B_n$ can uniquely be written as $g = \tau \cdot \sigma$ where $\tau \in \mathbb{R}^{n \times n}$ is a sign-change matrix and $\sigma \in \mathbb{R}^{n \times n}$ is a permutation matrix. Indeed, τ must then be the diagonal matrix whose i-th diagonal entry is 1 or -1 corresponding to the sign of the unique non-zero entry in the i-th row of g. For this choice of τ, the $\sigma := \tau^{-1} \cdot g$ is a permutation matrix. Analogously, we can also write each $g \in B_n$ uniquely as a product $g = \sigma \cdot \tau$ with σ a permutation matrix and τ a sign-change matrix (but these σ, τ are in general different from the σ, τ before).

Theorem 3.12. *The following n polynomials $p_1, \ldots, p_n \in K(\Lambda_2)$ form a set of generating rational invariants for the action of B_n on $\Lambda_2 = \{\sum_{i=1}^n \lambda_i x_i^2\}$:*

$$p_k := \lambda_1^k + \ldots + \lambda_n^k$$

for $k \in \{1, \ldots, n\}$.

Proof. By definition, a rational function $P \in K(\Lambda_2) = \mathbb{R}(\lambda_1, \ldots, \lambda_n)$ is a rational invariant for the action of B_n, i.e. $P \in K(\Lambda_2)^{B_n}$, if $P(v) = P(gv)$ for all $v \in \Lambda_2$ and $g \in B_n$. By Remark 3.11, this holds if and only if $P(v) = P(gv)\ \forall v \in \Lambda_2$ holds for permutation matrices g as well as for sign-change matrices g.

For a sign-change matrix g this is in fact always the case, since $gv = v$ for all $v \in \Lambda_2$. To see this, note that by Proposition 3.7 we only have to see that $g \operatorname{diag}(\lambda_1, \ldots, \lambda_n) g^T = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$ holds for all diagonal matrices g whose diagonal entries are ±1. This is clear.

On the other hand, permutation matrices act on quadratic forms of the type $v = \sum_{i=1}^n \lambda_i x_i^2$ simply by permuting the coefficients λ_i. Hence, a rational function $P \in K(\Lambda_2) = \mathbb{R}(\lambda_1, \ldots, \lambda_n)$ is a rational invariant if and only if it is symmetric in the variables $\lambda_1, \ldots, \lambda_n$. A version of the Fundamental Theorem of symmetric functions (see e.g. [**Stu08**, Proposition 1.1.2]) states that a rational function in n variables $\lambda_1, \ldots, \lambda_n$ which is symmetric with respect to those variables, can always be written as a rational expression in terms of the power sum polynomials $p_1, \ldots, p_n$ as defined above.[4] This shows the claim. □

We now know generating rational invariants $\{p_1, \ldots, p_n\}$ for $K(\Lambda_2)^{B_n}$, so by Corollary 3.4 the set $\{\rho^{-1}(p_1), \ldots, \rho^{-1}(p_n)\}$ is a set of generating rational invariants for the action of the orthogonal group on quadratic forms (where $\rho\colon K(V_2)^{O(n)} \xrightarrow{\cong} K(\Lambda_2)^{B_n}$ from Corollary 3.10). We now describe those "full" invariants explicitly.

Theorem 3.13. *Consider $V_2 = \{x^T A x \mid A = (a_{ij}) \in \mathbb{R}^{n \times n}$ symmetric$\}$. Then the following n polynomials $\tilde{p}_1, \ldots, \tilde{p}_n$ in the variables a_{ij} form a set of generating rational invariants for the action of $O(n)$ on V_2:*

$$\tilde{p}_k := \operatorname{Trace}(A^k)$$

for $k \in \{1, \ldots, n\}$.

Proof. First, we observe that $\tilde{p}_1, \ldots, \tilde{p}_n$ are indeed rational invariants for $O(n)$. By Proposition 3.7, for this we only have to check that $\operatorname{Trace}(A^k) = \operatorname{Trace}((gAg^T)^k)$ for all $g \in O(n)$. Indeed, this follows

[4] Typically, this result is stated in terms of polynomial expressions, not rational expressions. However, every symmetric rational expression can be written as a fraction of two symmetric polynomial expressions (see e.g. [**DK02**, Lemma 3.9.6]), so the version for rational expressions is implied by the more common version.

from $g^T = g^{-1}$, since $(gAg^{-1})^k = gA^kg^{-1}$ and $\mathrm{Trace}(gA^kg^{-1}) = \mathrm{Tr}(A^k)$ by general properties of the trace.

Now Corollary 3.4 proves the claim if we show that for any k the restriction of $\tilde{p}_k$ to Λ_2 is given by the expression p_k from Theorem 3.12. This is clear, since the trace of the matrix $\mathrm{diag}(\lambda_1, \ldots, \lambda_n)^k$ is precisely $\sum_{i=1}^n \lambda_i^k$. □

Example 3.14. We write out explicitly the generating rational invariants $\tilde{p}_i$ for $n = 2$ and $n = 3$. For $n = 2$ these expressions are

$$\tilde{p}_1 = \mathrm{Trace}\begin{pmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{pmatrix} = a_{11} + a_{22}$$

and

$$\tilde{p}_2 = \mathrm{Trace}\begin{pmatrix} a_{11}^2 + a_{12}^2 & a_{11}a_{12} + a_{12}a_{22} \\ a_{11}a_{12} + a_{12}a_{22} & a_{12}^2 + a_{22}^2 \end{pmatrix} = a_{11}^2 + 2a_{12}^2 + a_{22}^2.$$

Recall that in this notation, a binary quadratic form $v \in V_2$ is thought of as a triple $(a_{11}, a_{12}, a_{22}) \in \mathbb{R}^3$ forming the entries of the Gramian matrix $\begin{pmatrix} a_{11} & a_{12} \\ a_{12} & a_{22} \end{pmatrix}$, i.e. $v = a_{11}x^2 + 2a_{12}xy + a_{22}y^2$. Note that $\tilde{p}_1, \tilde{p}_2 \in K(V_2)^{O(2)}$ are precisely the invariants encountered in Example 2.3 (where we used instead the notation $a = a_{11}, b = a_{12}/2, c = a_{22}$).

For $n = 3$ we obtain the following expressions:

$$\begin{aligned}
\tilde{p}_1 &= a_{11} + a_{22} + a_{33}, \\
\tilde{p}_2 &= a_{11}^2 + 2a_{12}^2 + 2a_{13}^2 + a_{22}^2 + 2a_{23}^2 + a_{33}^2, \\
\tilde{p}_3 &= a_{11}^3 + 3a_{11}a_{12}^2 + 3a_{11}a_{13}^2 + 3a_{12}^2a_{22} + 6a_{12}a_{13}a_{23} + 3a_{13}^2a_{33} \\
&\qquad + a_{22}^3 + 3a_{22}a_{23}^2 + 3a_{23}^2a_{33} + a_{33}^3,
\end{aligned}$$

where we write elements of V_2 (i.e. ternary quadratic forms) as

$$a_{11}x^2 + 2a_{12}xy + a_{22}y^2 + 2a_{13}xz + 2a_{23}yz + a_{33}z^2.$$

Remark 3.15. It is worth emphasizing that the expressions $\tilde{p}_k$ in the variables a_{ij} can become quite large, as n grows larger. For the cases $n = 2$ and $n = 3$ this is not a relevant issue here, but once we pass from $2d = 2$ to higher degree $2d$, we will encounter the same phenomenon for $n = 2$ and $n = 3$ and it will quickly grow an important problem to resolve.

For example, for $n = 4$ the last invariant is

$$\begin{aligned}\tilde{p}_4 = a_{11}^4 &+ 4a_{11}^2a_{12}^2 + 4a_{11}^2a_{13}^2 + 4a_{11}^2a_{14}^2 + 4a_{11}a_{12}^2a_{22} + 8a_{11}a_{12}a_{13}a_{23} + 8a_{11}a_{12}a_{14}a_{24} \\
&+ 4a_{11}a_{13}^2a_{33} + 8a_{11}a_{13}a_{14}a_{34} + 4a_{11}a_{14}^2a_{44} + 2a_{12}^4 + 4a_{12}^2a_{13}^2 + 4a_{12}^2a_{14}^2 + 4a_{12}^2a_{22}^2 \\
&+ 4a_{12}^2a_{23}^2 + 4a_{12}^2a_{24}^2 + 8a_{12}a_{13}a_{22}a_{23} + 8a_{12}a_{13}a_{23}a_{33} + 8a_{12}a_{13}a_{24}a_{34} + 8a_{12}a_{14}a_{22}a_{24} \\
&+ 8a_{12}a_{14}a_{23}a_{34} + 8a_{12}a_{14}a_{24}a_{44} + 2a_{13}^4 + 4a_{13}^2a_{14}^2 + 4a_{13}^2a_{23}^2 + 4a_{13}^2a_{33}^2 + 4a_{13}^2a_{34}^2 \\
&+ 8a_{13}a_{14}a_{23}a_{24} + 8a_{13}a_{14}a_{33}a_{34} + 8a_{13}a_{14}a_{34}a_{44} + 2a_{14}^4 + 4a_{14}^2a_{24}^2 + 4a_{14}^2a_{34}^2 + 4a_{14}^2a_{44}^2 \\
&+ a_{22}^4 + 4a_{22}^2a_{23}^2 + 4a_{22}^2a_{24}^2 + 4a_{22}a_{23}^2a_{33} + 8a_{22}a_{23}a_{24}a_{34} + 4a_{22}a_{24}^2a_{44} + 2a_{23}^4 + 4a_{23}^2a_{24}^2 \\
&+ 4a_{23}^2a_{33}^2 + 4a_{23}^2a_{34}^2 + 8a_{23}a_{24}a_{33}a_{34} + 8a_{23}a_{24}a_{34}a_{44} + 2a_{24}^4 + 4a_{24}^2a_{34}^2 + 4a_{24}^2a_{44}^2 + a_{33}^4 \\
&+ 4a_{33}^2a_{34}^2 + 4a_{33}a_{34}^2a_{44} + 2a_{34}^4 + 4a_{34}^2a_{44}^2 + a_{44}^4,\end{aligned}$$

which is a polynomial with 55 terms. For higher values of n, the largest invariant $\tilde{p}_n$ consists of the following number of terms: 377 ($n = 5$), 3571 ($n = 6$), 40764 ($n = 7$), 552294 ($n = 8$), …[5]

Meanwhile, the invariants p_k from Theorem 3.12 (i.e. the restriction of $\tilde{p}_k$ to the slice) in the variables λ_i remain small: The expression p_k has only k terms. This is a first hint that instead of obtaining full expressions for rational invariants it can be more useful to just work with the information what their restriction to the slice is. We will again encounter this philosophy at several points later on.

Remark 3.16. All results in this section actually hold more generally in the setting of *polynomial invariants*. For example, the invariants described in Theorems 3.12 and 3.13 are in fact generating polynomial invariants, as introduced in Section 2.2 – even though this is not entirely clear from the approach presented in this section. Note that passing from $p_k \in K(\Lambda_2)^{B_n}$ to $\tilde{p}_k \in K(V_2)^{O(n)}$ does not introduce denominators as would be suggested by Remark 3.5. This should be viewed as a rather special property of the case of quadratic forms and will no longer be true in our treatment of the case $d > 2$.

3.3. A slice for higher degree

The aim of this section is to describe a slice $\Lambda_{2d} \subset V_{2d}$ for the action of $O(n)$ on V_{2d} for any $d \geq 1$. We will then use the constructed slice in Chapters 4 and 5 to construct invariants similar to the approach in Section 3.2.

For this, we have to start out with some basic facts about the apolar product and harmonic polynomials. First, we define an inner product $\langle v, w \rangle$ for $v, w \in V_{2d}$:

Definition 3.17. The **apolar inner product** $\langle , \rangle \colon V_{2d} \times V_{2d} \to \mathbb{R}$ is defined as follows: If $v = \sum_{i_1 \ldots i_n} a_{i_1 \ldots i_n} x_1^{i_1} \ldots x_n^{i_n} \in V_{2d}$ and $w =$

[5] This has been obtained by a straightforward use of the Computer Algebra Software *Maple*.

$\sum_{i_1\dots i_n} b_{i_1\dots i_n} x_1^{i_1} \dots x_n^{i_n} \in V_{2d}$, we define

$$\langle v, w\rangle := \sum_{i_1\dots i_n} i_1! \cdot \ldots \cdot i_n! \cdot a_{i_1\dots i_n} b_{i_1\dots i_n}.$$

We may make the same definition for $V_k := \mathbb{R}[x_1, \dots, x_n]_k$ for k odd. The importance of this inner product for the action of the orthogonal group is the fact that the group action of $O(n)$ preserves $\langle , \rangle$.

Proposition 3.18. *If $v, w \in V_{2d}$ (or, more generally, $v, w \in V_k$) and $g \in O(n)$, then $\langle gv, gw\rangle = \langle v, w\rangle$.*

Proof. *Step 1: The claim holds for V_1, i.e. the case of linear forms.*

Note that linear forms $v = \alpha_1 x_1 + \ldots + \alpha_n x_n \in V_1$ and $w = \beta_1 x_1 + \ldots + \beta_n x_n \in V_1$ can be written as $v = a^T x$ and $w = b^T x$, where $a = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \in \mathbb{R}^n$, $b = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} \in \mathbb{R}^n$ and we denote the vector of variables as $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$. Then, by definition, $\langle v, w\rangle = a^T b$. Note that $gv = a^T g^T x = (ga)^T x$ (and analogously for w), since the action of $O(n)$ is defined as the composition with $g^{-1} = g^T$. In particular,

$$\langle gv, gw\rangle = (ga)^T (gb) = a^T g^T g b = a^T b = \langle v, w\rangle$$

(using $g^T g = \mathrm{id}$).

Step 2: If $v_1, \dots, v_{2d} \in V_1$ and $w_1, \dots, w_{2d} \in V_1$ are linear forms and $v = v_1 \cdot \ldots \cdot v_{2d} \in V_{2d}$, $w = w_1 \cdot \ldots \cdot w_d \in V_{2d}$, then

$$\langle v, w\rangle = \sum_{\sigma \in \mathfrak{S}_{2d}} \langle v_1, w_{\sigma(1)}\rangle \cdot \ldots \cdot \langle v_{2d}, w_{\sigma(2d)}\rangle, \tag{3.3.1}$$

where the sum ranges over all permutations σ of the set $\{1, \dots, 2d\}$.

Note that the inner product on the left hand side is the apolar product for V_{2d}, while the inner products on the right hand side are the apolar product for V_1. Since the expressions of both sides are linear in each v_k and in each w_k, it is enough to show (3.3.1) for the case that each v_k and each w_k ranges over a given basis of V_1. As $x_1, \dots, x_n \in V_1$ form a basis of V_1, it is therefore enough to show:

$$\langle x_{i_1} \cdot \ldots \cdot x_{i_{2d}}, x_{j_1} \cdot \ldots \cdot x_{j_{2d}}\rangle = \sum_{\sigma \in \mathfrak{S}_{2d}} \langle x_{i_1}, x_{j_{\sigma(1)}}\rangle \cdot \ldots \cdot \langle x_{i_{2d}}, x_{j_{\sigma(2d)}}\rangle$$

holds for all $i_k, j_k \in \{1, \dots, n\}$. Using $\langle x_i, x_j\rangle = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{otherwise,} \end{cases}$, it is straightforward to check that both sides agree.

Step 3: $\langle gv, gw\rangle = \langle v, w\rangle$ holds for all $v, w \in V_{2d}$.

The claim is linear in v and linear in w, so it suffices to show it for $v = x_1^{i_1} \dots x_n^{i_n}$ and $w = x_1^{j_1} \dots x_n^{j_n}$ (where $i_1 + \dots + i_n = 2d$ and $j_1 + \dots + j_n = 2d$). This special case is an immediate consequence of combining Step 1 and Step 2. This concludes the proof. □

Notation 3.19. From now on, for fixed n we denote

$$Q := x_1^2 + \dots + x_n^2 \in V_2.$$

This $Q \in V_2$ plays a special role, since the following holds (more or less immediately by definition of $O(n)$):

Observation 3.20. *The action of $O(n)$ on V_2 fixes Q, i.e. $gQ = Q$ for all $g \in O(n)$. To see this, note that the Gramian matrix of $Q = x_1^2 + \dots + x_n^2 \in V_2$ is the identity matrix, hence the Gramian matrix of $gQ \in V_2$ is $g \cdot \mathrm{id} \cdot g^T = \mathrm{id}$ by Proposition 3.7, showing $gQ = Q$.*

Definition 3.21. For any $d \geq 1$ we consider the inclusion of vector spaces

$$V_{2d-2} \hookrightarrow V_{2d}, \quad v \mapsto Q \cdot v.$$

and its image $QV_{2d-2} \subset V_{2d}$, which is given by those polynomials $v \in V_{2d}$ which are divisible by Q.

We now define the subspace $\mathcal{H}_{2d} \subset V_{2d}$ of **harmonic polynomials** of degree $2d$ to be the orthogonal complement of $QV_{2d-2} \subset V_{2d}$ with respect to the apolar inner product on V_{2d}.

A consequence of Proposition 3.18 is the following:

Proposition 3.22. *Let $g \in O(n)$ and $v \in V_{2d}$. Then the following holds:*

(i) If $v \in QV_{2d-2} \subset V_{2d}$, then also $gv \in QV_{2d-2}$.
(ii) If $v \in \mathcal{H}_{2d}$, then also $gv \in \mathcal{H}_{2d}$.

Proof. (i) We can write $v = Q \cdot v'$ for $v' \in V_{2d-2}$. By Observation 3.20, we have $gv = (gQ) \cdot (gv') = Q \cdot (gv') \in QV_{2d-2}$.

(ii) We have to show that $\langle gv, w \rangle = 0$ for all $w \in QV_{2d-2} \subset V_{2d}$. We have $\langle gv, w \rangle = \langle v, g^{-1}w \rangle$ by Proposition 3.18, and $g^{-1}w \in V_{d-1} \subset V_{2d}$ follows from part (i). Since $v \in \mathcal{H}_d$ is orthogonal on QV_{2d-2}, this concludes the proof.

□

By Definition 3.21 there is an orthogonal decomposition $V_{2d} = \mathcal{H}_{2d} \oplus QV_{2d-2}$. Since we can also decompose V_{2d-2} in this manner, we can iterate this decomposition which leads to the following observation.

Observation 3.23 (Harmonic Decomposition)**.** *For $d \geq 1$ there is a decomposition*

$$V_{2d} = \mathcal{H}_{2d} \oplus Q\mathcal{H}_{2d-2} \oplus Q^2\mathcal{H}_{2d-4} \cdots \oplus Q^{d-2}\mathcal{H}_4 \oplus Q^{d-1}V_2,$$

i.e. each $v \in V_{2d}$ can uniquely be written as a sum

$$v = h_{2d} + Qh_{2d-2} + Q^2h_{2d-4} + \ldots + Q^{d-2}h_4 + Q^{d-1}v'$$

where $h_{2k} \in \mathcal{H}_{2k}$ and $v' \in V_2$.

Warning 3.24. Recall that $V_{2d} = \mathcal{H}_{2d} \oplus QV_{2d-2}$ is a decomposition into orthogonal subspaces with respect to the apolar inner product. In contrast, the decomposition in Observation 3.23 is *not* an orthogonal decomposition if $2d > 4$. This is due to the fact that $\langle v, w\rangle = \langle Qv, Qw\rangle$ does *not* hold for $v, w \in V_{2d-2}$. On the other hand, it remains true that each of the subspaces in the Harmonic Decomposition are preserved under each element g of $O(n)$ as in Proposition 3.22.

Remark 3.25. In the literature, harmonic functions are typically introduced in a different way than presented here, and then it is shown that they have the properties described above. For more background, we refer to the literature on Harmonic Functions, e.g. [**ABW01**].

Definition 3.26. For $d \geq 1$ and $n \geq 2$ we consider the Harmonic Decomposition of V_{2d} from Observation 3.23 and define $\Lambda_{2d} \subset V_{2d}$ to be the subspace

$$\Lambda_{2d} := \mathcal{H}_{2d} \oplus Q\mathcal{H}_{2d-2} \oplus \cdots \oplus Q^{d-2}\mathcal{H}_4 \oplus Q^{d-1}\Lambda_2,$$

where $\Lambda_2 \subset V_2$ is the subspace of quadratic forms with diagonal Gramian matrix as in Definition 3.8.

Remark 3.27. In other words, elements of the subspace Λ_{2d} are those $v \in V_{2d}$ which can be written as

$$v = h_{2d} + Qh_{2d-2} + Q^2h_{2d-4} + \ldots + Q^{d-2}h_4 + Q^{d-1}v'$$

with $h_{2k} \in \mathcal{H}_{2k}$ and $v' \in \Lambda_2$. Note that for $2d = 2$ this definition agrees with Definition 3.8.

Proposition 3.28. *Let $d \geq 1$. The subspace $\Lambda_{2d} \subset V_{2d}$ is a slice for the action of $O(n)$ on V_{2d} and its stabilizer is the group $B_n \subset O(n)$ of signed permutation matrices. In particular, there is a one-to-one correspondence between rational invariants*

$$\rho \colon K(V_{2d})^{O(n)} \xrightarrow{\cong} K(\Lambda_{2d})^{B_n}$$

which is given by restriction of rational functions.

Proof. The second statement is a consequence of the first statement by Theorem 3.2.

If

$$v = h_{2d} + Qh_{2d-2} + Q^2h_{2d-4} + \ldots + Q^{d-2}h_4 + Q^{d-1}v'$$

is the Harmonic Decomposition of an element $v \in V_{2d}$ (see Observation 3.23), then the Harmonic Decomposition of gv is

$$gv = (gh_{2d}) + Q(gh_{2d-2}) + \ldots + Q^{d-2}(gh_4) + Q^{d-1}(gv').$$

This follows from Observation 3.20 and Proposition 3.22.

From this observation, the claim is an immediate consequence of the fact that $\Lambda_2 \subset V_2$ is a slice for the action of $O(n)$ on V_2 with stabilizer B_n – see Proposition 3.9. □

CHAPTER 4

Invariants for binary forms ($n = 2$)

In this chapter, we will use the results from Section 3.3 to construct a set of generating rational invariants for V_{2d} in the case $n = 2$. By Proposition 3.28, this amounts to determining rational invariants for the action of the subgroup $B_2 \subset O(2)$ on Λ_{2d}. Since Λ_{2d} is defined by means of the Harmonic Decomposition of V_{2d}, a main step consists in understanding the subspaces $\mathcal{H}_{2d} \subset V_{2d}$ and finding an appropriate description how the subgroup $B_2 \subset O(2)$ acts on $\mathcal{H}_{2d}$. This will be the done in Section 4.1. This will be the foundation for describing rational invariants in Section 4.2.

Throughout this chapter, we fix $n = 2$.

4.1. Binary harmonic polynomials and the B_2-action

We start out with a characterization of the elements in the subspace $\mathcal{H}_{2d} \subset V_{2d}$.

Lemma 4.1. *Let $d \geq 1$. A binary form*

$$v = \sum_{i=0}^{2d} \binom{2d}{i} a_i x^{2d-i} y^i \in V_{2d}$$

is contained in $\mathcal{H}_{2d}$ if and only if $a_{i-1} + a_{i+1} = 0$ holds for all $i \in \{1, \ldots, 2d-1\}$.

Proof. By definition, v lies in $\mathcal{H}_{2d}$ if and only if $\langle v, (x^2+y^2)w \rangle = 0$ for all $w \in V_{2d-2}$. Since the monomials $x^{d-j-1}y^{j-1}$ for $j \in \{1, \ldots, d-1\}$ form a basis of V_{2d-2}, we may restrict to the cases that w is any of these monomials. We have

$$\langle v, (x^2+y^2)x^{2d-j-1}y^{j-1} \rangle = \left\langle \sum_{i=0}^{2d} \binom{2d}{i} a_i \cdot x^{2d-i}y^i, (x^2+y^2)x^{2d-j-1}y^{j-1} \right\rangle$$
$$= \binom{d}{j-1} a_{j-1}(2d-j+1)!(j-1)! + \binom{2d}{j+1} a_{j+1}(2d-j-1)!(j+1)!$$
$$= (2d)! \cdot (a_{j-1} + a_{j+1}),$$

where we used that

$$\langle x^k y^\ell, x^{k'} y^{\ell'} \rangle = \begin{cases} k!\ell! & \text{if } k = k', \ell = \ell' \\ 0 & \text{otherwise.} \end{cases}$$

Hence $v \in \mathcal{H}_{2d}$ if and only if $a_{j-1} + a_{j+1} = 0$ for all $j \in \{1, \dots, n\}$. □

An immediate consequence of Lemma 4.1 is that $\dim \mathcal{H}_{2d} = 2$ for all $d \geq 1$. More precisely, we can specify a very convenient basis:

Proposition 4.2. *Let $d \geq 1$. The two polynomials*

$$u_{2d-1} := \sum_{\substack{i=0 \\ i \text{ odd}}}^{2d} (-1)^{\frac{i-1}{2}} \binom{2d}{i} x^{2d-i} y^i,$$

$$u_{2d} := \sum_{\substack{i=0 \\ i \text{ even}}}^{2d} (-1)^{\frac{i}{2}} \binom{2d}{i} x^{2d-i} y^i$$

form an orthogonal basis of $\mathcal{H}_{2d}$ with respect to the apolar product.

Proof. Lemma 4.1 shows $u_{2d-1} \in \mathcal{H}_{2d}$ and $u_{2d} \in \mathcal{H}_{2d}$. If $v = \sum_{i=0}^{2d} \binom{2d}{i} a_i x^{2d-i} y^i \in \mathcal{H}_{2d}$, then Lemma 4.1 implies that

$$a_i = \begin{cases} (-1)^{\frac{i}{2}} a_0 & \text{if } i \text{ even,} \\ (-1)^{\frac{i-1}{2}} a_1 & \text{if } i \text{ odd,} \end{cases}$$

hence $v = a_1 u_{2d-1} + a_0 u_{2d}$. Since u_{2d-1} and u_{2d} do not have any monomials in common, their apolar product is $\langle u_{2d-1}, u_{2d} \rangle = 0$ by definition. □

Additionally to the above u_k, we define $u_0 := 1 \in V_0$. Note that for $k \geq 0$ the polynomial expression u_k has degree k (if k is even) or $k+1$ (if k is odd).

Example 4.3. The first nine u_k are the following expressions:

$$\begin{aligned} &u_0 = 1 && \\ &u_1 = 2xy && u_2 = x^2 - y^2 \\ &u_3 = 4x^3y - 4xy^3 && u_4 = x^4 - 6x^2y^2 + y^4 \\ &u_5 = 6x^5y - 20x^3y^3 + 6xy^5 && u_6 = x^6 - 15x^4y^2 + 15x^2y^4 - y^6 \\ &u_7 = 8x^7y - 56x^5y^3 + 56x^3y^5 - 8xy^7 && u_8 = x^8 - 28x^6y^2 + 70x^4y^4 - 28x^2y^6 + y^8 \end{aligned}$$

The Harmonic Decomposition from Observation 3.23 implies that those u_i form a basis for V_{2d} after multiplying them with a suitable power of $Q = x^2 + y^2$. Precisely:

Proposition 4.4. *Let $d \geq 1$. Then the expressions*

$$u_i^{(2d)} := (x^2 + y^2)^{d - \lceil \frac{i}{2} \rceil} \cdot u_i \in V_{2d}$$

for $i \in \{0, 1, \dots, 2d\}$ form a basis for V_{2d}. A basis for the subspace $\Lambda_{2d} \subset V_{2d}$ is given by the same expressions for $i \in \{0, 2, 3, \dots, 2d\}$ (i.e. leaving out $u_1^{(2d)}$).

Proof. Let $Q := x^2 + y^2 \in V_2$. In Observation 3.23, we noted that

$$V_{2d} = \mathcal{H}_{2d} \oplus Q\mathcal{H}_{2d-2} \oplus Q^2\mathcal{H}_{2d-4} \cdots \oplus Q^{d-2}\mathcal{H}_4 \oplus Q^{d-1}V_2.$$

By definition of $\mathcal{H}_2$, we also have $V_2 = \mathcal{H}_2 \oplus QV_0$, so

$$V_{2d} = \mathcal{H}_{2d} \oplus Q\mathcal{H}_{2d-2} \oplus Q^2\mathcal{H}_{2d-4} \cdots \oplus Q^{d-2}\mathcal{H}_4 \oplus Q^{d-1}\mathcal{H}_2 \oplus Q^dV_0.$$

Note that $u_0 = 1$ is a basis of the one-dimensional vector space V_0 and recall that u_{2k-1} and u_{2k} form a basis of $\mathcal{H}_{2k}$ (for all $k \geq 1$) by Proposition 4.2. From this, we conclude that $u_i^{(2d)}$ for $i \in \{0, 1, \dots, 2d\}$ form a basis of V_{2d}.

To show that $u_i^{(2d)}$ for $i \neq 1$ form a basis for Λ_{2d}, recall that by definition

$$\Lambda_{2d} := \mathcal{H}_{2d} \oplus Q\mathcal{H}_{2d-2} \oplus \cdots \oplus Q^{d-2}\mathcal{H}_4 \oplus Q^{d-1}\Lambda_2.$$

Hence, it is enough to show this claim for $d = 1$.

If $v \in \Lambda_2$, then $v = ax^2 + by^2$ for some $a, b \in \mathbb{R}$ by definition of Λ_2. Then

$$v = \frac{a+b}{2} \cdot (x^2 + y^2) + \frac{a-b}{2}(x^2 - y^2) = \frac{a+b}{2} \cdot Qu_0 + \frac{a-b}{2}u_2.$$

This shows that $u_0^{(2)} = Qu_0$ and $u_2^{(2)} = u_2$ form a basis for Λ_2, concluding the proof. □

Remark 4.5. As in Warning 3.24, it should be noted that the above is *not* an orthogonal basis of V_{2d} for the apolar product, in contrast to Proposition 4.2.

The main reason why we work with this particular basis $u_i^{(2d)}$ is that it also reveals easily how the group $B_2 \subset O(2)$ acts on Λ_{2d} (resp. V_{2d}):

Lemma 4.6. *Let $d \geq 1$.*

(i) The group $B_2 \subset O(2)$ is generated by

$$g_1 := \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \in B_2 \quad \text{and} \quad g_2 := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in B_2,$$

i.e. each element of B_2 can be written as a successive product of the elements g_1 and g_2.

(ii) If $v = \sum_{i=0}^{2d} \alpha_i u_i^{(2d)} \in V_{2d}$ (for some $\alpha_0, \dots, \alpha_{2d} \in \mathbb{R}$), then

$$g_1 v = \sum_{i=0}^{2d} (-1)^i \alpha_i u_i^{(2d)} \quad \text{and} \quad g_2 v = \sum_{i=0}^{2d} (-1)^{\binom{i}{2}} \alpha_i u_i^{(2d)}.$$

Proof. (i) By Remark 3.11, every element of B_2 can be written as a product of a 2×2 permutation matrix and a 2×2 sign change matrix. The only non-trivial 2×2 permutation matrix is g_1, so it remains to see that all non-trivial matrices of the form $\operatorname{diag}(\tau_1, \tau_2)$

with $\tau_1, \tau_2 = \pm 1$ can be written as a successive product of g_1 and g_2. We check this explicitly:

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = g_1, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = g_2 g_1 g_2, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = g_1 g_2 g_1 g_2.$$

(ii) Since $Q = x^2 + y^2$ satisfies $gQ = Q$ for all $g \in B_2$ and because of linearity, it suffices to show that $g_1 u_i = (-1)^i u_i$ and $g_2 u_i = (-1)^{\binom{i}{2}} u_i$ holds for all $i \in \{0, 1, \dots, d\}$.

By definition of the action of $B_2 \subset O(2)$, the polynomial expression $g_1 u_i$ arises from the polynomial expression u_i by substituting the variable x by $-x$. From the definition of u_i it is then immediate that $g_1 u_i = u_i$ if i is even and $g_1 u_i = -u_i$ if i is odd (compare also Example 4.3). In short, $g_1 = (-1)^i u_i$.

In the same way, the polynomial expression $g_2 u_i$ by definition arises from the polynomial expression u_i by interchanging the variables x and y. The definition of u_i is such that $g_2 u_i = u_i$ if $i \equiv 0$ or $1 \pmod 4$ and $g_2 u_i = -u_i$ if $i \equiv 2$ or $3 \pmod 4$. In short, $g_2 u_i = (-1)^{\binom{i}{2}} u_i$.

□

4.2. Invariants for binary forms

Theorem 4.7. *Let $d \geq 2$. Considering*

$$\Lambda_{2d} = \left\{ \sum_{\substack{0 \leq i \leq 2d \\ i \neq 1}} \alpha_i u_i^{(2d)} \mid \alpha_0, \alpha_2, \alpha_3, \dots, \alpha_{2d} \in \mathbb{R} \right\},$$

the following $2d$ rational functions $p_k \colon \Lambda_{2d} \dashrightarrow \mathbb{R}$ are generating rational invariants for $K(\Lambda_{2d})^{B_2}$.

$$p_k \left(\sum_{i \neq 1} \alpha_i u_i^{(2d)} \right) := \begin{cases} \alpha_k & \textit{if } k \equiv 0 \pmod 4, \\ \alpha_2 \alpha_3 \alpha_k & \textit{if } k \equiv 1 \pmod 4, \\ \alpha_2 \alpha_k & \textit{if } k \equiv 2 \pmod 4, \\ \alpha_3 \alpha_k & \textit{if } k \equiv 3 \pmod 4 \end{cases}$$

for $k \in \{0, 2, 3, \dots, 2d\}$.

Proof. *Step 1: The expressions $p_k \in K(\Lambda_{2d})$ are rational invariants for the action of B_2.*

We have to check that $p_k(v) = p_k(gv)$ holds for all $g \in B_2$, $v \in \Lambda_{2d}$. By Lemma 4.6.(i), it is enough to check this for the two generators $g = g_1$ and $g = g_2$ from Lemma 4.6.

Let $v = \sum_{i\neq 1} \alpha_i u_i^{(2d)}$. Then by Lemma 4.6.(ii) we have

$$\begin{aligned}
p_k(g_1 v) &= p_k\left(\sum_{i\neq 1}(-1)^i \alpha_i u_i^{(2d)}\right)\\
&= \begin{cases} (-1)^k\alpha_k = \alpha_k & \text{if } k \equiv 0 \pmod 4,\\ ((-1)^2\alpha_2)((-1)^3\alpha_3)(-1)^k\alpha_k = \alpha_2\alpha_3\alpha_k & \text{if } k \equiv 1 \pmod 4,\\ ((-1)^2\alpha_2)((-1)^k\alpha_k) = \alpha_2\alpha_k & \text{if } k \equiv 2 \pmod 4,\\ ((-1)^3\alpha_3)((-1)^k\alpha_k) = \alpha_3\alpha_k & \text{if } k \equiv 3 \pmod 4 \end{cases}\\
&= p_k(v).
\end{aligned}$$

Analogously,

$$\begin{aligned}
p_k(g_2 v) &= p_k\left(\sum_{i\neq 1}(-1)^{\binom{i}{2}} \alpha_i u_i^{(2d)}\right)\\
&= \begin{cases} (-1)^{\binom{k}{2}}\alpha_k = \alpha_k & \text{if } k \equiv 0 \pmod 4,\\ ((-1)^{\binom{2}{2}}\alpha_2)((-1)^{\binom{3}{2}}\alpha_3)(-1)^{\binom{k}{2}}\alpha_k = \alpha_2\alpha_3\alpha_k & \text{if } k \equiv 1 \pmod 4,\\ ((-1)^{\binom{2}{2}}\alpha_2)((-1)^{\binom{k}{2}}\alpha_k) = \alpha_2\alpha_k & \text{if } k \equiv 2 \pmod 4,\\ ((-1)^{\binom{3}{2}}\alpha_3)((-1)^{\binom{k}{2}}\alpha_k) = \alpha_3\alpha_k & \text{if } k \equiv 3 \pmod 4 \end{cases}\\
&= p_k(v).
\end{aligned}$$

This shows that the p_k are rational invariants for the action of B_2.

Step 2: $p_0, p_2, p_3, \dots, p_{2d} \in K(V_{2d})^{B_2}$ form a set of generating rational invariants.

Let $q \in K(V_{2d})^{B_2}$, i.e. $q\left(\sum_{i\neq 1}\alpha_i u_i^{(2d)}\right)$ is a rational expression $q = \frac{q_1}{q_0} \in \mathbb{R}(\alpha_0, \alpha_2, \alpha_3, \dots, \alpha_{2d})$ in the variables $\alpha_0, \alpha_2, \alpha_3, \dots, \alpha_{2d}$ which stays invariant under the action of B_2. For $k \in \{0, 4, 5, \dots, 2d\}$ we can replace each occurrence of α_k as follows:

$$\alpha_k = \begin{cases} p_k & \text{if } k \equiv 0 \pmod 4,\\ \frac{p_k}{\alpha_2\alpha_3} & \text{if } k \equiv 1 \pmod 4,\\ \frac{p_k}{\alpha_2} & \text{if } k \equiv 2 \pmod 4,\\ \frac{p_k}{\alpha_3} & \text{if } k \equiv 3 \pmod 4. \end{cases}$$

This way, we rewrite q as a rational expression in the invariants p_k and the remaining variables α_2 and α_3. Using $p_2 = \alpha_2^2$ and $p_3 = \alpha_3^2$, we can also replace higher powers of the variables α_2 and α_3 accordingly such that we are left with an expression

$$q = \frac{r_1 + r_2\alpha_2 + r_3\alpha_3 + r_4\alpha_2\alpha_3}{r_5 + r_6\alpha_2 + r_7\alpha_3 + r_8\alpha_2\alpha_3},$$

where $r_1, \dots, r_8 \in \mathbb{R}[p_0, p_2, p_3, \dots, p_{2d}]$ are polynomial expressions in p_k.

After multiplying the numerator and denominator with $(r_5+r_6\alpha_2)-\alpha_3(r_7+r_8\alpha_2)$, the new denominator contains the variable α_3 only as α_3^2, so after simplifying the entire resulting expression again by replacing higher powers of α_2 and α_3 as before, we are left with an expression where α_3 does not show up anymore in the denominator:

$$q = \frac{r_9 + r_{10}\alpha_2 + r_{11}\alpha_3 + r_{12}\alpha_2\alpha_3}{r_{13} + r_{14}\alpha_2}$$

for $r_9, \ldots, r_{14}$ some polynomial expressions in the invariants p_k.

Extending numerator and denominator by the factor $r_{13} - r_{14}\alpha_2$ and replacing $\alpha_2^2 = p_2$, we have finally rewritten

$$q = r_{15} + r_{16}\alpha_2 + r_{17}\alpha_3 + r_{18}\alpha_2\alpha_3,$$

where $r_{15}, \ldots, r_{18} \in \mathbb{R}(p_0, p_2, p_3, \ldots, p_{2d})$ are rational expressions in the invariants p_k.

Being expressions in p_k, the $r_{15}, \ldots, r_{18}$ are themselves rational invariants for the action of B_2. In particular, acting by $g_2 \in B_2$ from Lemma 4.6 leaves $r_{15}, \ldots, r_{18}$ invariant while replacing α_2 by $-\alpha_2$ and α_3 by $-\alpha_3$ (according to part (ii) of Lemma 4.6). Hence:

$$q(g_2 v) = r_{15} - r_{16}\alpha_2 - r_{17}\alpha_3 + r_{18}\alpha_2\alpha_3.$$

Since q is a rational invariant, we have $q(g_2 v) = q(v)$, from which we deduce the equality

$$r_{15} + r_{16}\alpha_2 + r_{17}\alpha_3 + r_{18}\alpha_2\alpha_3 = r_{15} - r_{16}\alpha_2 - r_{17}\alpha_3 + r_{18}\alpha_2\alpha_3.$$

Hence, $r_{16}\alpha_2 + r_{17}\alpha_3 = 0$, i.e. $q = r_{15} + r_{18}\alpha_2\alpha_3$.

In the same way, we now get

$$r_{15} + r_{18}\alpha_2\alpha_3 = q(v) = q(g_1 v) = r_{15} - r_{18}\alpha_2\alpha_3,$$

i.e. $r_{18}\alpha_2\alpha_3 = 0$. This shows $q = r_{15}$, i.e. we have expressed an arbitrary rational invariant $q \in K(\Lambda_{2d})^{B_2}$ as a rational expression (namely the expression r_{15}) in terms of $p_0, p_2, p_3, \ldots, p_{2d}$. This shows that those p_k form a set of generating rational invariants. □

With the Slice Lemma (Theorem 3.2) we conclude the following:

Corollary 4.8. *Let $d \geq 2$. Then there is a set of $2d$ generating rational invariants $\tilde{p}_0, \tilde{p}_2, \tilde{p}_3, \ldots, \tilde{p}_{2d} \in K(V_{2d})^{O(2)}$ for the action of $O(2)$ on V_{2d} such that their restriction to the subspace Λ_{2d} is given by $\tilde{p}_k|_{\Lambda_{2d}} = p_k$ (and this property characterizes $\tilde{p}_k$ uniquely).*

CHAPTER 5

Invariants for ternary forms ($n = 3$)

In this chapter, we will construct a set of generating rational invariants for V_{2d} in the case $n = 3$, $d \geq 2$. As in the previous chapter, it is essential to find an appropriate basis for $\mathcal{H}_{2d}$ with respect to which the action of the group $B_3 \subset O(3)$ on the space Λ_{2d} becomes apparent. Based on that, we will be able to describe invariants. We will first examine the case of ternary quartics, i.e. $2d = 4$, in Sections 5.1 and 5.2. This is the first relevant case for applications that cannot be modeled with quadratic forms; at the same time the treatment of this case serves as a model for the case of higher degree, since it already reflects most phenomena encountered for $2d > 4$. We turn to the general case of any $d \geq 2$ in Sections 5.3 and 5.4.

Throughout this chapter, we fix $n = 3$.

5.1. Ternary quartic harmonic functions and the action of B_3

Throughout this section, we consider the case $d = 2$, i.e. degree $2d = 4$. We are therefore concerned with the vector space $V_4 = \mathbb{R}[x, y, z]_4$ of ternary quartic forms which decomposes according to Observation 3.23 as $V_4 = \mathcal{H}_4 \oplus QV_2$ (where $Q = x^2 + y^2 + z^2$). By Proposition 3.28, we are interested in the action of $B_3 \subset O(3)$ on the subspace $\Lambda_4 = \mathcal{H}_4 \oplus Q\Lambda_2$. To this end, we start out by providing a useful basis for the vector space $\mathcal{H}_4$:

Proposition 5.1. *The following nine ternary quartic forms form a basis for the $\mathbb{R}$-vector space $\mathcal{H}_4$:*

$$u_{1,0}^{(4)} := 6x^2yz - y^3z - yz^3,\ u_{1,1}^{(4)} := y^4 - 6y^2z^2 + z^4,\ u_{1,2}^{(4)} := y^3z - yz^3,$$
$$u_{2,0}^{(4)} := 6y^2zx - z^3x - zx^3,\ u_{2,1}^{(4)} := z^4 - 6z^2x^2 + x^4,\ u_{2,2}^{(4)} := z^3x - zx^3,$$
$$u_{3,0}^{(4)} := 6z^2xy - x^3y - xy^3,\ u_{3,1}^{(4)} := x^4 - 6x^2y^2 + y^4,\ u_{3,2}^{(4)} := x^3y - xy^3.$$

Warning 5.2. These $u_{i,j}^{(4)}$ – defined in the setting $n = 3$ – are unrelated to the expressions $u_k^{(2d)}$ defined in Section 4.1 for the setting $n = 2$. No confusion should arise from this, as we are only concerned with the case $n = 3$ in this chapter.

Proof. From $\dim V_4 = \binom{3+4-1}{4} = 15$ and $\dim V_2 = \binom{3+2-1}{2} = 6$ and the Harmonic Decomposition $V_4 = \mathcal{H}_4 \oplus QV_2$, it follows that $\mathcal{H}_4$

is a 9-dimensional $\mathbb{R}$-vector space. Therefore, it suffices to check that that all $u_{i,j}^{(4)}$ ($i \in \{1,2,3\}$, $j \in \{0,1,2\}$) are linearly independent and that they are contained in the subspace $\mathcal{H}_4$ of V_4.

Let $\sum_{i=1}^{3}\sum_{j=0}^{2}\lambda_{i,j}u_{i,j}^{(4)} = 0$ for some $\lambda_{i,j} \in \mathbb{R}$. By considering the coefficient of the monomials y^2z^2, z^2x^2 and x^2y^2 in the expression $\sum_{i=1}^{3}\sum_{j=1}^{3}\lambda_{i,j}u_{i,j}^{(4)}$, we see that $\lambda_{1,1}$, $\lambda_{2,1}$ and $\lambda_{3,1}$ must be zero. Similarly, the coefficients of x^2yz, y^2zx and z^2xy reveal $\lambda_{1,0} = \lambda_{2,0} = \lambda_{3,0} = 0$. Now, we are left with $\sum_{i=1}^{3}\lambda_{i,2}u_{i,2}^{(4)} = 0$, from which we deduce $\lambda_{1,2} = \lambda_{2,2} = \lambda_{3,2} = 0$ by considering the coefficients of y^3z, z^3x and x^3y. Therefore all $\lambda_{i,j}$ must be zero. This shows that the $u_{i,j}^{(4)}$ are linearly independent.

It remains to show that $u_{i,j}^{(4)} \in \mathcal{H}_4$ for all i, j. By the Definition 3.21, $\mathcal{H}_4$ is the orthogonal complement of QV_2 in V_4 with respect to the apolar product. Hence, we only need to see that $\langle u_{i,j}^{(4)}, Qv\rangle = 0$ for $v \in \{x^2, y^2, z^2, xy, yz, zx\}$. It is straightforward to check this. □

The above proof does not provide much insight to how and why the above basis was chosen in this particular way. Below, we will see that the action of B_3 on $\mathcal{H}_4$ is described easily with respect to this basis, but the question how to come up with this basis remains. We will address this question later on in Section 5.3, where we systematically examine the case of higher degree ($d > 2$). For the purpose of approaching the case $d = 2$ the above statement shall be enough.

Definition 5.3. Additionally to the above, we define

$$u_{1,3}^{(4)} := Qx^2, \quad u_{2,3}^{(4)} := Qy^2, \quad u_{3,3}^{(4)} := Qz^2,$$

where $Q = x^2 + y^2 + z^2$.

Corollary 5.4. *The expressions $u_{i,j}^{(4)}$ for $i \in \{1,2,3\}, j \in \{0,1,2,3\}$ form a basis for Λ_4.*

Proof. This follows immediately from Proposition 5.1 because of $\Lambda_4 = \mathcal{H}_4 \oplus Q\Lambda_2$. □

Lemma 5.5. *Let $v = \sum_{i=1}^{3}\sum_{j=0}^{4}\alpha_{i,j}u_{i,j}^{(4)} \in \Lambda_4$ (for some $\alpha_{i,j} \in \mathbb{R}$).*

(i) If $g \in B_3$ is a 3×3 permutation matrix and σ is the permutation of $\{1,2,...,n\}$ corresponding to g, then

$$gv = \sum_{i=1}^{3}\sum_{j=0}^{4}\operatorname{sgn}(\sigma)^{\zeta(j)}\alpha_{i,j}u_{\sigma(i),j}^{(4)},$$

where $\operatorname{sgn}(\sigma) = \det(g)$ *is the* signum *of the permutation σ and*

$$\zeta(j) := \begin{cases} 1 & \text{if } j = 2, \\ 0 & \text{otherwise} \end{cases}$$

for $j \in \{0,1,2,3\}$.

(ii) *If* $g = \operatorname{diag}(\tau_1,\tau_2,\tau_3) \in B_3$ *(where* $\tau_i = \pm 1$*) is a* 3×3 *sign-change matrix, then*

$$gv = \sum_{i=1}^{3}\sum_{j=0}^{4}(\tau_1\tau_2\tau_3\tau_i)^{j+1}\alpha_{i,j}u_{i,j}^{(4)}.$$

Proof. (i) The element g acts by permuting the variables x, y and z in the polynomial expression $v \in \Lambda_4 \subset \mathbb{R}[x,y,z]_4$. From the definition of $u_{i,j}$ we can read off that this permutation of variables gives

$$gu_{i,j}^{(4)} = \begin{cases} \operatorname{sgn}(\sigma)u_{\sigma(i),j}^{(4)} & \text{if } j = 2,\\ u_{\sigma(i),j}^{(4)} & \text{otherwise,}\end{cases}$$

from which the claim follows by linearity.

(ii) By the definition of the group action, the element $g \in B_3$ acts on a polynomial expression $v \in V_4 = \mathbb{R}[x,y,z]_4$ by simply substituting x by $\tau_1 x$, y by $\tau_2 y$, and z by $\tau_3 z$. From the definition of $u_{i,j}$ we then see that for $j \in \{1,3\}$ we have

$$gu_{1,j}^{(4)} = \tau_2\tau_3u_{1,j}^{(4)}, \quad gu_{2,j}^{(4)} = \tau_1\tau_3u_{2,j}^{(4)}, \quad gu_{3,j}^{(4)} = \tau_1\tau_2u_{3,j}^{(4)},$$

and for $j \in \{0,2\}$ we have $gu_{i,j}^{(4)} = u_{i,j}^{(4)}$. The claim above is just a reformulation of this.

□

5.2. Invariants for ternary quartic forms

In this section, we use the basis for Λ_4 constructed in Section 5.1 to explicitly determine generating rational invariants for $K(\Lambda_4)^{B_3}$. We proceed in the spirit of Section 4.2, even though in this case ($n = 3$) the constructed invariants will be slightly more involved than in the previous case ($n = 2$).

Theorem 5.6. *A set of generating rational invariants for* $K(\Lambda_4)^{B_3}$ *is given by the* 12 *rational functions* $p_{i,j} \colon \Lambda_4 \dashrightarrow \mathbb{R}$ *for* $i \in \{1,2,3\}$, $j \in \{0,1,2,3\}$ *whose value at* $v = \sum_{i,j}\alpha_{i,j}u_{i,j}^{(4)} \in \Lambda_4$ *is given by*

$$\begin{aligned} p_{1,0}(v) &:= \alpha_{1,0}^2 + \alpha_{2,0}^2 + \alpha_{3,0}^2,\\ p_{2,0}(v) &:= \alpha_{1,0}\alpha_{2,0}\alpha_{3,0},\\ p_{3,0}(v) &:= \alpha_{1,0}^4 + \alpha_{2,0}^4 + \alpha_{3,0}^4. \end{aligned}$$

and the remaining $p_{i,j}(v)$ *are given by the matrix product*

$$\begin{pmatrix} p_{1,1}(v) & p_{1,2}(v) & p_{1,3}(v)\\ p_{2,1}(v) & p_{2,2}(v) & p_{2,3}(v)\\ p_{3,1}(v) & p_{3,2}(v) & p_{3,3}(v)\end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 1 & 1\\ \alpha_{1,0}^2 & \alpha_{2,0}^2 & \alpha_{3,0}^2\\ \alpha_{1,0}^4 & \alpha_{2,0}^4 & \alpha_{3,0}^4\end{pmatrix}}_{=:M(\alpha)} \cdot \underbrace{\begin{pmatrix} \alpha_{1,1} & \alpha_{1,2}\alpha_{1,0}\det M(\alpha) & \alpha_{1,3}\\ \alpha_{2,1} & \alpha_{2,2}\alpha_{2,0}\det M(\alpha) & \alpha_{2,3}\\ \alpha_{3,1} & \alpha_{3,2}\alpha_{3,0}\det M(\alpha) & \alpha_{3,3}\end{pmatrix}}_{=:A(\alpha)}.$$

Remark 5.7. Note that the occurring factor $\det M(\alpha)$ is explicitly given as

$$\det M(\alpha) = (\alpha_{1,0}^2 - \alpha_{2,0}^2)(\alpha_{2,0}^2 - \alpha_{3,0}^2)(\alpha_{3,0}^2 - \alpha_{1,0}^2).$$

Proof. *Step 1: The expressions $p_{i,j} \in K(\Lambda_4)$ are rational invariants for the action of B_3.*

By Remark 3.11, it suffices to show $p_{i,j}(gv) = p_{i,j}(v)$ $\forall v \in \Lambda_4$ in the case that $g \in B_3$ is a permutation matrix or a sign-change matrix. It is a straightforward task to check this using Lemma 5.5. (We can use Remark 5.7 to see that the expression $\det M(\alpha)$ remains unchanged under the action any sign-change matrix g and is mapped to $(-1)^{\det g} \cdot \det M(\alpha)$ if g is a permutation matrix.)

Step 2: If $q \in K(\Lambda_4)^{B_3}$ is an invariant whose value at $v = \sum_{i,j} \alpha_{i,j} u_{i,j}^{(4)}$ is given by a polynomial *expression in $\alpha_{1,0}, \alpha_{2,0}, \alpha_{3,0}$ only, then q can be written polynomially in terms of $p_{1,0}, p_{2,0}, p_{3,0}$.*

First, we consider the monomials $\alpha_{1,0}^i \alpha_{2,0}^j \alpha_{3,0}^k$ of the polynomial expression q. By Lemma 5.5, a sign-change matrix $\operatorname{diag}(\tau_1, \tau_2, \tau_3) \in B_3$ acts on q by replacing $\alpha_{1,0}^i \alpha_{2,0}^j \alpha_{3,0}^k$ by

$$\tau_1^{j+k} \tau_2^{i+k} \tau_3^{i+j} \cdot \alpha_{1,0}^i \alpha_{2,0}^j \alpha_{3,0}^k,$$

so q can only be invariant with respect to all sign-change matrices if for all its monomials $\alpha_{1,0}^i \alpha_{2,0}^j \alpha_{3,0}^k$, the numbers $i+j$, $i+k$ and $j+k$ are even numbers, i.e. $i \equiv j \equiv k \pmod 2$. In particular, we can write q as a polynomial in

$$p_{2,0} := \alpha_{1,0}\alpha_{2,0}\alpha_{3,0}, \quad \beta_1 := \alpha_{1,0}^2, \quad \beta_2 := \alpha_{2,0}^2, \quad \beta_3 := \alpha_{3,0}^2.$$

If $g \in B_3$ is a permutation matrix and σ is the permutation of $\{1,2,3\}$ corresponding to g, then g acts according to Lemma 5.5 on q by replacing β_i by β_{σ_i}. Therefore, g is an symmetric polynomial expression in the three variables $\beta_1, \beta_2, \beta_3$. By the Fundamental Theorem of symmetric functions, see [**Stu08**, Proposition 1.1.2], q can therefore be written as a polynomial expression in the three power sum polynomials

$$\begin{aligned} &\beta_1 + \beta_2 + \beta_3 = p_{1,0}, \\ &\beta_1^2 + \beta_2^2 + \beta_3^2 = p_{3,0} \text{ and} \\ &\beta_1^3 + \beta_2^3 + \beta_3^3 = \frac{3}{2} p_{1,0} p_{3,0} - \frac{1}{2} p_{1,0}^3 + 3 p_{2,0}^2. \end{aligned}$$

With this, we have expressed q as a polynomial expression in terms of $p_{1,0}, p_{2,0}, p_{3,0}$.

Step 3: If $q \in K(\Lambda_4)^{B_3}$ is an invariant whose value at $v = \sum_{i,j} \alpha_{i,j} u_{i,j}^{(4)}$ is given by a rational *expression in $\alpha_{1,0}, \alpha_{2,0}, \alpha_{3,0}$ only, then q can be written as a rational expression in terms of $p_{1,0}, p_{2,0}, p_{3,0}$.*

It is enough to show that the rational expression q can be written as $q = \frac{q_1}{q_0}$ such that q_1 and q_0 are polynomial expressions which are also invariants, because we may express both q_0 and q_1 as polynomial expressions in terms of $p_{1,0}, p_{2,0}, p_{3,0}$. We may assume that the polynomial expressions q_1 and q_0 have no common factor. Since $q = \frac{q_1}{q_0}$ is an invariant, we have for each $g \in B_3$:

$$q_1(gv) \cdot q_0(v) = q_1(v) \cdot q_0(gv), v \in \Lambda_4.$$

Since $q_0(v)$ and $q_1(v)$ have no common factor, the same is true for $q_1(gv)$ and $q_0(gv)$ (as polynomial expressions in $\alpha_{1,0}, \alpha_{2,0}, \alpha_{3,0}$). Therefore, we deduce from the above equation that for each $g \in B_3$ there exists a scalar $\lambda_g \in \mathbb{R}^*$ such that $q_1(gv) = \lambda_g q_1(v)$ and $q_0(gv) = \frac{1}{\lambda_g} q_0(v)$ holds for all $v \in \Lambda_4$. Note that for each $g \in B_3$ we have $g^k = \mathrm{id}$ for some $k \geq 1$, hence $q_1(v) = q_1(g^k v) = \lambda_g^k q_1(v)$, which shows $\lambda_g = \pm 1$. Note that we therefore have

$$q_1(gv)q_0(gv) = q_1(v)q_0(v), \quad q_0(gv)^2 = q_0(v)^2 \quad \forall g \in B_3, v \in \Lambda_4.$$

In particular, $q = \frac{q_1 q_0}{q_0^2}$ writes q as a fraction whose numerator and denominator are both invariants.

Step 4: If $q \in K(\Lambda_4)^{B_3}$, then q can be written as a rational expression in the invariants $p_{i,j}$.

The invariant q is a rational expression in the variables $\alpha_{i,j}$. We observe that

$$\begin{pmatrix} \alpha_{1,1} & \alpha_{1,2}\alpha_{1,0} \det M(\alpha) & \alpha_{1,3} \\ \alpha_{2,1} & \alpha_{2,2}\alpha_{2,0} \det M(\alpha) & \alpha_{2,3} \\ \alpha_{3,1} & \alpha_{3,2}\alpha_{3,0} \det M(\alpha) & \alpha_{3,3} \end{pmatrix} = M(\alpha)^{-1} \cdot \begin{pmatrix} p_{1,1}(v) & p_{1,2}(v) & p_{1,3}(v) \\ p_{2,1}(v) & p_{2,2}(v) & p_{2,3}(v) \\ p_{3,1}(v) & p_{3,2}(v) & p_{3,3}(v) \end{pmatrix},$$

where $M(\alpha)$ is an expression only involves the variables $\alpha_{1,0}, \alpha_{2,0}, \alpha_{3,0}$. With this, we can replace each occurrence of $\alpha_{i,j}$ for $i, j \in \{1, 2, 3\}$ by a rational expression involving the different invariants $p_{i,j}$ as well as the three variables $\alpha_{1,0}, \alpha_{2,0}, \alpha_{3,0}$. Since the $p_{i,j}$ are invariant under the action of B_3, we may just consider them as constants and we can then rewrite the remaining rational invariant involving only $\alpha_{1,0}, \alpha_{2,0}, \alpha_{3,0}$ in terms of $p_{1,0}, p_{2,0}, p_{3,0}$ by Step 3. This concludes the proof of Step 4, showing that the $p_{i,j}$ as defined above form a set of generating rational invariants for the action of B_3. □

With the Slice Lemma (Theorem 3.2) we conclude:

Corollary 5.8. *There is a set of 12 generating rational invariants $\tilde{p}_{i,j} \in K(V_{2d})^{O(2)}$ (for $i \in \{1, 2, 3\}, j \in \{0, 1, 2, 3\}$) for the action of $O(3)$ on V_4 such that their restriction to the subspace Λ_4 is given by $\tilde{p}_{i,j}|_{\Lambda_4} = p_{i,j}$ (and this property characterizes $p_{i,j}$ uniquely).*

5.3. The action of B_3 for higher degree – formulation

We now turn to the case of arbitrary even degree $2d \geq 4$. The structure of the B_3-action on Λ_{2d} remains very similar to what we saw in the special case $d = 2$. The main result is the construction of a convenient basis for Λ_{2d}, providing the following structural description analogous to Lemma 5.5.

Proposition 5.9. *Let $d \geq 2$ be not divisible by 3. Then* $\dim \Lambda_{2d} = 3(k+1)$ *for some $k \in \mathbb{N}$. There exists a basis $(u_{i,j}^{(2d)})_{1\leq i\leq 3, 0\leq j\leq k}$ of Λ_{2d} and mappings $\xi, \zeta\colon \{0,\dots,k\} \to \{0,1\}$ with $\xi(0) = 1, \zeta(0) = 0$ such that the action of B_3 on Λ_{2d} is given as follows: Let $v = \sum_{i=1}^{3}\sum_{j=0}^{k} \alpha_{i,j} u_{i,j}^{(2d)} \in \Lambda_{2d}$.*

(i) If $g \in B_3$ is a 3×3 permutation matrix and σ is the permutation of $\{1, 2, ..., n\}$ corresponding to g, then

$$gv = \sum_{i=1}^{3}\sum_{j=0}^{k} \operatorname{sgn}(\sigma)^{\zeta(j)} \alpha_{\sigma(i),j} u_{i,j}^{(2d)},$$

where $\operatorname{sgn}(\sigma) = \det(g) = \pm 1$ *is the signum of the permutation σ.*

(ii) If $g = \operatorname{diag}(\tau_1, \tau_2, \tau_3) \in B_3$ (where $\tau_i = \pm 1$) is a 3×3 sign-change matrix, then

$$gv = \sum_{i=1}^{3}\sum_{j=0}^{k} (\tau_1\tau_2\tau_3\tau_i)^{\xi(j)} \alpha_{i,j} u_{i,j}^{(2d)}.$$

We also need to consider the case that d is divisible by 3.

Proposition 5.10. *Let d be a multiple of 3. Then*

$$\dim \Lambda_{2d} = 3(k+1) + 1$$

for some $k \in \mathbb{N}$. There exists a basis $u_\infty^{(2d)}, (u_{i,j}^{(2d)})_{1\leq i\leq 3, 0\leq j\leq k}$ of Λ_{2d} and mappings $\xi, \zeta\colon \{0,\dots,k\} \to \{0,1\}$ with $\xi(0) = 1, \zeta(0) = 0$ such that the action of B_3 on Λ_{2d} is given exactly as in Proposition 5.9 on the basis elements $u_{i,j}^{(2d)}$, and on the additional basis element $u_\infty^{(2d)}$ given by

$$gu_\infty^{(2d)} = u_\infty^{(2d)} \quad \textit{for all } g \in B_3.$$

We will delay the (technical) constructive proof for these two results to Section 5.5. This allows us to immediately formulate the results about rational invariants analogous to Theorem 5.6.

5.4. Invariants for higher degree ternary forms

Theorem 5.11. *Let $d \geq 2$ be not divisible by 3 and consider the notations from Proposition 5.9.*

A set of generating rational invariants for $K(\Lambda_{2d})^{B_3}$ is given by the $3(k+1)$ rational functions $p_{i,j}\colon \Lambda_{2d} \dashrightarrow \mathbb{R}$ for $i \in \{1,2,3\}$, $j \in \{0,1,\dots,k\}$ whose value at $v=\sum_{i,j}\alpha_{i,j}u_{i,j}^{(2d)} \in \Lambda_{2d}$ is given by

$$\begin{aligned} p_{1,0}(v) &:= \alpha_{1,0}^2+\alpha_{2,0}^2+\alpha_{3,0}^2,\\ p_{2,0}(v) &:= \alpha_{1,0}\alpha_{2,0}\alpha_{3,0},\\ p_{3,0}(v) &:= \alpha_{1,0}^4+\alpha_{2,0}^4+\alpha_{3,0}^4. \end{aligned}$$

and the remaining $p_{i,j}(v)$ are the entries of the $3\times k$-matrix given as the matrix product

$$\begin{pmatrix} p_{1,1}(v) & \dots & p_{1,k}(v)\\ p_{2,1}(v) & \dots & p_{2,k}(v)\\ p_{3,1}(v) & \dots & p_{3,k}(v)\end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 1 & 1\\ \alpha_{1,0}^2 & \alpha_{2,0}^2 & \alpha_{3,0}^2\\ \alpha_{1,0}^4 & \alpha_{2,0}^4 & \alpha_{3,0}^4\end{pmatrix}}_{=:M(\alpha)} \cdot A(\alpha),$$

where $A(\alpha)$ is the $3\times k$-matrix whose (i,j)-th entry is

$$A(\alpha)_{i,j} = \alpha_{i,j}\alpha_{i,0}^{\xi(j)}(\det M(\alpha))^{\zeta(j)}.$$

Theorem 5.12. *Let d be a multiple of 3 and consider the notations from Proposition 5.10. We define $3(k+1)$ rational functions $p_{ij}\colon \Lambda_{2d} \dashrightarrow \mathbb{R}$ whose value at $v=\alpha_\infty u_\infty^{(2d)}+\sum_{i,j}\alpha_{i,j}u_{i,j}^{(2d)} \in \Lambda_{2d}$ is given by the same expressions as above (i.e. not involving α_∞), and add the rational function $p_\infty \in K(\Lambda_{2d})$ given by $p_\infty(v) := \alpha_\infty$. Then those $3(k+1)+1$ rational functions $p_\infty, p_{i,j}$ form a set of generating rational invariants for $K(\Lambda_{2d})^{B_3}$.*

Proof of Theorems 5.11 and 5.12. The proof is completely analogous to the proof of Theorem 5.6. □

5.5. The action of B_3 for higher degree – construction

In this section, we give the construction of a basis of Λ_{2d} with the properties specified in Propositions 5.9 and 5.10. First, we establish a result analogous to Lemma 4.1.

Notation 5.13. For nonnegative integers i,j,k and $r=i+j+k$, we denote the *multinomial*

$$\binom{r}{i,j,k} := \frac{r!}{i!j!k!}.$$

Furthermore, we recall that the binomial $\binom{r}{k}$ is defined for all integers $k \geq 0$ and $r \in \mathbb{Z}$ – even if $r<k$ or if r is even negative –, as

$$\binom{r}{k} := \frac{r(r-1)\cdot\ldots\cdot(r-k+1)}{k!}.$$

Lemma 5.14. *Let $d \geq 2$. A ternary form*

$$v = \sum_{i+j+k=2d} \binom{2d}{i,j,k} a_{i,j,k} x^i y^j z^k \in V_{2d}$$

is contained in $\mathcal{H}_{2d}$ if and only if $a_{i+2,j,k} + a_{i,j+2,k} + a_{i,j,k+2} = 0$ holds for all $i,j,k \in \mathbb{N}$ such that $i+j+k = 2d-2$.

Proof. The proof is analogous to the proof of Lemma 4.1, but we choose to provide it in detail nevertheless. By definition, v lies in $\mathcal{H}_{2d}$ if and only if $\langle v, Qw\rangle = 0$ for all $w \in V_{2d-2}$, where $Q = x^2+y^2+z^2 \in V_2$. Since the monomials $x^iy^jz^k$ for all i,j,k such that $i+j+k = 2d-2$ form a basis of V_{2d-2}, we may restrict to the cases that w is any of these monomials. We have

$$\begin{aligned}&\langle v, Qx^iy^jz^k\rangle \\ &= \left\langle \sum_{i'+j'+k'=d} \binom{2d}{i',j',k'} a_{i',j',k'} x^{i'}y^{j'}z^{k'}, (x^2+y^2+z^2)x^iy^jz^k \right\rangle \\ &= (2d)! \cdot (a_{i+2,j,k} + a_{i,j+2,k} + a_{i,j,k+2}),\end{aligned}$$

where we used that

$$\langle x^{i'}y^{j'}z^{k'}, x^iy^jz^k\rangle = \begin{cases} i!j!k! & \text{if } i=i', j=j', k=k' \\ 0 & \text{otherwise.}\end{cases}$$

Hence $v \in \mathcal{H}_{2d}$ if and only if $a_{i+2,j,k} + a_{i,j+2,k} + a_{i,j,k+2} = 0$ for all $i,j,k \in \mathbb{N}$ such that $i+j+k = 2d-2$. □

Recall that $\dim V_{2d} = \binom{2d+n-1}{n-1} = \binom{2d+2}{2}$, so that $\dim \Lambda_{2d} = \binom{2d+2}{2} - 3$. Note that $\dim \mathcal{H}_{2d} = \dim V_{2d} - \dim V_{2d-2} = 4d+1$. With this, we are prepared for the construction of an "appropriate" basis for Λ_{2d}.

Proof of Propositions 5.9 and 5.10. We simultaneously prove both propositions by induction on $d \geq 2$. The case $d = 2$ has been established in Corollary 5.4 and Lemma 5.5. We now consider the case $d > 2$ and we may assume Proposition 5.9 resp. Proposition 5.10 for $d-1$. In particular, we have elements $u_{i,j}^{(2d-2)} \in \Lambda_{2d-2}$ for $1 \leq i \leq 3, 0 \leq j < r_0$, where $r_0 := \left\lfloor \frac{\dim \Lambda_{2d-2}}{3} \right\rfloor = \left\lfloor \frac{1}{3}\binom{2d}{2} \right\rfloor - 1$ (and also an element $u_\infty^{(2d-2)} \in \Lambda_{2d-2}$ if $d \equiv 1 \pmod 3$).

By Definition 3.26, we have

$$\Lambda_{2d} = \mathcal{H}_{2d} \oplus Q\Lambda_{2d-2},$$

where $Q = x^2+y^2+z^2 \in V_2$.

Hence, as a first step, we define

$$u_{i,j}^{(2d)} := Qu_{i,j}^{(2d-2)} \quad \forall 1 \leq i \leq 3, 0 \leq j \leq r_0 - 1.$$

If $d \not\equiv 1 \pmod 3$, then these $u_{i,j}^{(2d)}$ already form a basis for the subspace $Q\Lambda_{2d-2} \subset \Lambda_{2d}$ (with the desired properties) and it only remains to extend it by a suitable basis of $\mathcal{H}_{2d}$. If $d \equiv 1 \pmod 3$, we need to extend it by a basis of $\mathcal{H}_{2d} \oplus \langle Qu_\infty^{(2d-2)} \rangle$.

Step 1: Definition of additional $u_{3,j}^{(2d)}$ for $j \geq r_0$

(1) For $\ell \in \{0, 1, \dots, d-1\}$, we define

$$u_{3,r_0+\ell}^{(2d)} := \sum_{i+j+k=2d} \binom{2d}{i,j,k} a_{i,j,k} x^i y^j z^k,$$

with $a_{i,j,k}$ given as follows: If $\ell + d$ is even, the entries $a_{i,j,k}$ are defined as

$$a_{i,j,k} := 0 \qquad \text{if } i \text{ even or } j \text{ even or } k \text{ odd,}$$
$$a_{2i+1,2j+1,2k} := \begin{cases} (-1)^k & \text{if } k \leq \ell \text{ and } i - j = \ell - k + 1, \\ (-1)^{k+1} & \text{if } k \leq \ell \text{ and } j - i = \ell - k + 1, \\ 0 & \text{otherwise.} \end{cases}$$

In the other case that $\ell + d$ is an odd number, the entries $a_{i,j,k}$ are for $\ell > 0$ defined as

$$a_{i,j,k} := 0 \qquad \text{if } i \text{ even or } j \text{ even or } k \text{ odd,}$$
$$a_{2i+1,2j+1,2k} := \begin{cases} (-1)^k \cdot 2 & \text{if } k = \ell \text{ and } i = j, \\ (-1)^k & \text{if } k < \ell \text{ and } |j - i| = \ell - k, \\ 0 & \text{otherwise,} \end{cases}$$

and for $\ell = 0$ as

$$a_{i,j,k} := \begin{cases} (-1)^{\frac{i-1}{2}} & \text{if } k = 0,\ i \text{ and } j \text{ odd} \\ 0 & \text{otherwise.} \end{cases}$$

This defines $u_{3,j}^{(2d)}$ for $r_0 \leq j < r_1$, where $r_1 := r_0 + d$. [1]

(2) For $\ell \in \{0, 1, \dots, \left\lfloor \frac{d+1}{3} \right\rfloor - 1\}$, we define $u_{3,r_1+\ell}^{(2d)}$ to be the element $\sum_{i+j+k=2d} \binom{2d}{i,j,k} a_{i,j,k} x^i y^j z^k$ given as follows: If $\ell + d$ is odd, the entries $a_{i,j,k}$ are defined as

$$a_{i,j,k} := 0 \qquad \text{if one of } i, j, k \text{ is odd,}$$
$$a_{2i,2j,2k} := \begin{cases} (-1)^i \cdot \binom{\frac{i-j-k+\ell-1}{2}}{\ell-k} & \text{if } k \leq \ell, \\ 0 & \text{otherwise.} \end{cases}$$

[1] Apart from the special case $\ell = 0$, d odd, these expressions are obtained by defining $a_{t,2d-t,0} = \pm a_{2d-t,t,0} = \pm 1$ for one odd number t (specifically, $t = d + \ell + 1$ resp. $t = d + \ell$), defining the remaining $a_{i,j,0}$ and $a_{i,j,1}$ to be zero, and iteratively computing the remaining $a_{i,j,k}$ from the equations in Lemma 5.14.

In the other case that $\ell + d$ is an even number, the entries $a_{i,j,k}$ are defined as

$$a_{i,j,k} := 0 \qquad \text{if one of } i,j,k \text{ is odd,}$$

$$a_{2i,2j,2k} := \begin{cases} (-1)^i \cdot \binom{\frac{i-j-k+\ell}{2}}{\ell-k} + (-1)^i \cdot \binom{\frac{i-j-k+\ell}{2}-1}{\ell-k} & \text{if } k \le \ell, \\ 0 & \text{otherwise.} \end{cases}$$

This defines $u_{3,j}^{(2d)}$ for $r_1 \le j < r_2$, where $r_2 := r_1 + \left\lfloor \frac{d+1}{3} \right\rfloor$. If $d \equiv 2 \pmod 3$, this finishes "Step 1". [2]

(3) If $d \equiv 1 \pmod 3$, we add

$$u_{3,r_2}^{(2d)} := Qu_{\infty}^{(2d-2)} + \sum_{i+j+k=2d} \binom{2d}{i,j,k} a_{i,j,k} x^i y^j z^k,$$

where the entries $a_{i,j,k}$ are defined precisely as in (2) for $\ell = \left\lfloor \frac{d+1}{3} \right\rfloor$.

(4) If $d \equiv 0 \pmod 3$, we add $u_{\infty}^{(2d)} := \sum_{i+j+k=2d} \binom{2d}{i,j,k} a_{i,j,k} x^i y^j z^k$, where the entries $a_{i,j,k}$ are given as follows:

$$a_{i,j,k} := 0 \qquad \text{if one of } i,j,k \text{ is odd,}$$

$$a_{2i,2j,2k} := \begin{cases} (-1)^{\left(\frac{|j-k|-i+d/3}{2}\right)} \cdot \binom{\frac{|j-k|-i+d/3}{2}}{d/3-i} & \text{if } i < d/3, \\ (-1)^{\left(\frac{|i-k|-j+d/3}{2}\right)} \cdot \binom{\frac{|i-k|-j+d/3}{2}}{d/3-j} & \text{if } j < d/3, \\ (-1)^{\left(\frac{|i-j|-k+d/3}{2}\right)} \cdot \binom{\frac{|i-j|-k+d/3}{2}}{d/3-k} & \text{if } k < d/3, \\ 2 & \text{if } i = j = k = d/3. \end{cases}$$

Note that the cases specified above overlap, but nevertheless, this expression is well-defined: If both $i < d/3$ and $j < d/3$, we must have $k = d - i - j > d/3$ and then

$$|j-k| - i = k - j - i = |i-k| - j.$$

The cases where both $i < d/3$ and $k < d/3$, or that both $j < d/3$ and $k < d/3$ are analogous. [3]

We have now constructed $u_{3,j}^{(2d)}$ for $r_0 \le j < r$, where $r = r_2 + 1$ (if $d \equiv 1 \pmod 3$) or $r = r_2$ (otherwise). Precise counting in the above constructions reveals

$$r = \left\lfloor \frac{1}{3} \binom{2d+2}{2} \right\rfloor - 1 = \left\lfloor \frac{\dim \Lambda_d}{3} \right\rfloor.$$

[2] These expressions $u_{3,r_1+\ell}^{(2d)}$ were obtained by first defining $a_{2i,2d-2\ell-2i,2\ell} := \pm 1$ (alternatingly) and $a_{2i,2j,2k} = 0$ for all $k > \ell$, and then completing this to a harmonic function by computing the $a_{2i,2j,2k}$ for $k < \ell$ with the use of the equations in Lemma 5.14 – in a way that preserves the symmetry $a_{2i,2j,2k} = a_{2j,2i,2k}$ or the anti-symmetry $a_{2i,2j,2k} = -a_{2j,2i,2k}$.

[3] This expressions $u_{\infty}^{(2d)}$ was obtained by defining $a_{d/3,d/3,d/3} := 2$ and completing this to a harmonic function with the use of the equations in Lemma 5.14 in such a way that the values $a_{i,j,k}$ are symmetric with respect to i,j,k.

This concludes Step 1.

Step 2: Definition of $u_{1,j}^{(2d)}$ and $u_{2,j}^{(2d)}$ for $j \geq r_0$

In Step 1, we have defined $u_{3,j}^{(2d)}$ for $r_0 \leq j < r$. We define $u_{1,j}^{(2d)}$ and $u_{2,j}^{(2d)}$ analogously, with the variables x, y, z interchanged (cyclicly). We make this precise:

Let $g_0 := \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \in B_3$. This group element acts as follows: If $v \in V_{2d} = \mathbb{R}[x, y, z]_{2d}$, then $g_0 v \in V_{2d}$ arises from the polynomial expression v by cyclicly substituting x by y, y by z, and z by x. We defined $u_{3,j}^{(2d)}$ for $j \geq r_0$ in Step 1. We now simply define:

$$u_{1,j}^{(2d)} := g_0 u_{3,j}^{(2d)} \qquad \text{and } u_{2,j}^{(2d)} := g_0 u_{1,j}^{(2d)}$$

for all $r_0 \leq j < r$. This finishes the construction of $u_{i,j}^{(2d)}$ (and $u_\infty^{(2d)}$), and it remains to show that they form a basis of Λ_{2d} and have the desired properties regarding the B_3-action.

Step 3: These $u_{i,j}^{(2d)} \in V_{2d}$, $1 \leq i \leq 3, 0 \leq j < r$ (together with $u_\infty^{(2d)}$ if d is a multiple of 3) are contained in Λ_{2d}.

Recall that $\Lambda_{2d} = \mathcal{H}_{2d} \oplus Q\Lambda_{2d-2}$. By definition, we know that $u_{i,j}^{(2d)} = Qu_{i,j}^{(2d-2)} \in Q\Lambda_{2d-2}$ for $j < r_0$. The expressions $u_{3,j}^{(2d)} \in V_{2d}$ for $r_0 \leq j < r_2$ can be checked to be contained in $\mathcal{H}_{2d} \subset V_{2d}$ with the criterion from Lemma 5.14 (in fact, the coefficients $a_{i,j,k}$ in the construction of $u_{3,j}^{(2d)}$ in Step 1 were carefully chosen such that this holds true).

For illustration, we show that $u_{3,j}^{(2d)} \in \mathcal{H}_{2d}$ in the case $j = r_1 + \ell$ and $\ell + d$ odd, as considered in (2) of Step 1. By Lemma 5.14, we have to check that

$$a_{2(i+1),2j,2k} + a_{2i,2(j+1),2k} + a_{2i,2j,2(k+1)} = 0.$$

This is straightforward:

$$\begin{aligned} & a_{2(i+1),2j,2k} + a_{2i,2(j+1),2k} + a_{2i,2j,2(k+1)} \\ & = (-1)^{i+1} \cdot \binom{\frac{i-j-k+\ell}{2}}{\ell - k} + (-1)^i \cdot \binom{\frac{i-j-k+\ell-2}{2}}{\ell - k} + (-1)^i \cdot \binom{\frac{i-j-k+\ell-2}{2}}{\ell - k - 1} \\ & \overset{(*)}{=} (-1)^{i+1} \cdot \binom{\frac{i-j-k+\ell}{2}}{\ell - k} + (-1)^i \cdot \binom{\frac{i-j-k+\ell-2}{2} + 1}{\ell - k} = 0, \end{aligned}$$

where in $(*)$, we used the formula $\binom{N}{K} = \binom{N-1}{K1} + \binom{N-1}{K-1}$. Proving $u_{3,j}^{(2d)} \in \mathcal{H}_{2d}$ in the other cases works in the same way. Since $g_0 \in B_3 \subset O(3)$, Proposition 3.22 then implies $u_{i,j}^{(2d)} \in \mathcal{H}_{2d}$ for all $i \in \{1, 2, 3\}$.

For the special constructions (3) and (4) from Step 1 it can equally be checked using Lemma 5.14 that $u_{i,r_2}^{(2d)} - Qu_\infty^{(2d-2)} \in \mathcal{H}_{2d}$ if $d \equiv 1$

(mod 3) and that $u_\infty^{(2d)} \in \mathcal{H}_{2d}$ if $d \equiv 0 \pmod 3$. This concludes Step 3.

Step 4: The $u_{i,j}^{(2d)} \in \Lambda_{2d}$, $1 \le i \le 3, 0 \le j < r$ (together with $u_\infty^{(2d)}$ if d is a multiple of 3) form a basis of Λ_{2d}.

Recall that $\dim \Lambda_{2d} = 3r+1$ if d is a multiple of 3 and that $\dim \Lambda_{2d} = 3r$ otherwise, so the number of $u_{i,j}^{(2d)}$ (and $u_\infty^{(2d)}$) equals the dimension of Λ_{2d}. Therefore, it suffices to show that they are linearly independent. By induction, we already know that $u_{i,j}^{(2d)} = Qu_{i,j}^{(2d-2)}$ for $j < r_0$ are linearly independent, so because of $\Lambda_{2d} = \mathcal{H}_{2d} \oplus \Lambda_{2d-2}$, it suffices to show that the rest is also linearly independent

For this, assume that $\sum_{i=1}^3 \sum_{j=r_0}^{r-1} \lambda_{i,j} u_{i,j}^{(2d)} = 0$ (or $\sum_{i,j} \lambda_{i,j} u_{i,j}^{(2d)} + \lambda_\infty u_\infty = 0$ if d is a multiple of 3). In the case that d is a multiple of 3, note that in this expression the coefficient of the monomial $x^{d/3} y^{d/3} z^{d/3}$ is precisely $2\lambda_\infty$ (since $a_{d/3,d/3,d/3} = 0$ for all of the $u_{i,j}^{(2d)}$), so we must have $\lambda_\infty = 0$. Hence we are in all cases left with

$$\sum_{i=1}^{3} \sum_{j=r_0}^{r-1} \lambda_{i,j} u_{i,j}^{(2d)} = 0.$$

If not all $\lambda_{3,j}$ for $r_0 \le j < r_1$ are zero, we may consider the largest $\ell < r_1 - r_0$ such that $\lambda_{3,r_0+\ell} \neq 0$. Then we observe from the construction of the $u_{i,j}^{(2d)}$ that in the expression $\sum_{i,j} \lambda_{i,j} u_{i,j}^{(2d)}$, the coefficient of the monomial $x^{2i+1,2j+1,2\ell}$ is a non-zero multiple of $\lambda_{3,r_0+\ell}$ (for a suitable choice of i,j). This is a contradiction to $\lambda_{3,r_0+\ell} \neq 0$, showing that all $\lambda_{3,j} = 0$ for $r_0 \le j < r_1$. The same of course holds for $\lambda_{1,j}$ and $\lambda_{2,j}$.

Hence, we are left with

$$\sum_{i=1}^{3} \sum_{j=r_1}^{r-1} \lambda_{i,j} u_{i,j}^{(2d)} = 0.$$

If not all $\lambda_{i,j}$ for $r_1 \le j < r_2$ are zero, we consider the largest $\ell < r_2 - r_1$ such that $\lambda_{i,r_1+\ell} \neq 0$ for some i. We may assume by symmetry that $\lambda_{3,r_1+\ell} \neq 0$. Because of $\ell < r_2 - r_1 = \left\lfloor \frac{d+1}{3} \right\rfloor$, there exist i,j such that $i + j + \ell = d/2$ and $i,j > \ell$. We consider the coefficient of the monomial $x^{2i} y^{2j} z^{2\ell}$ in $\sum_{i,j} \lambda_{i,j} u_{i,j}^{(2d)}$. By maximality of ℓ, it is immediate from the construction in Step 1 that this is a non-zero multiple of $\lambda_{3,r_1+\ell}$. This contradicts $\lambda_{3,r_1+\ell} \neq 0$, so all $\lambda_{i,j}$ for $r_1 \le j < r_2$ must be zero.

If $d \not\equiv 1 \pmod 3$, this shows that all $\lambda_{i,j} = 0$, so we proved linear independence. In the case $d \equiv 1 \pmod 3$, we are still left with

$$\sum_{i=1}^{3} \lambda_{i,r_2} u_{1,r_2}^{(2d)} = 0.$$

Recall that the construction of u_{i,r_2} (see (3) of Step 1) involves $Qu_\infty^{(2d-2)}$. Because of $\Lambda_{2d} = \mathcal{H}_{2d} \oplus Q\Lambda_{2d-2}$, we must have

$$\left(\sum_{i=1}^{3} \lambda_{i,r_2}\right) Qu_\infty^{(2d-2)} = 0$$

(i.e. $\sum_{i=1}^{3} \lambda_{i,r_2} = 0$) as well as

$$\sum_{i=1}^{3} \lambda_{i,r_2}(u_{i,r_2}^{(2d)} - Qu_\infty^{(2d-2)}) = 0.$$

Considering the coefficients of $x^{(d+4)/3}y^{(d+4)/3}z^{(d-2)/3}$ and $x^{(d+4)/3}y^{(d-2)/3}z^{(d+4)/3}$ in the latter expression gives

$$\lambda_{1,r_2} - \lambda_{2,r_2} = 0 \quad \text{and} \quad \lambda_{1,r_1} - \lambda_{2,r_3} = 0,$$

hence $\lambda_{1,r_2} = \lambda_{2,r_2} = \lambda_{3,r_2}$. Since we also have $\sum_{i=1}^{3} \lambda_{i,r_2} = 0$, this shows that all $\lambda_{i,r_2} = 0$, also concluding the case $d \equiv 1 \pmod 3$.

Step 5: The group B_3 acts with respect to this basis as claimed.

On the basis elements $u_{i,j}^{(2d)} = Qu_{i,j}^{(2d-2)}$ for $j < r_0$, we know this by induction, since $gQ = Q$ for all $g \in B_3$. (Here, we are defining $\xi(j) = \pm 1$ and $\zeta(j) = \pm 1$ to take the same values for $2d$ as for $2d-2$.)

If $g = \operatorname{diag}(\tau_1, \tau_2, \tau_3) \in B_3$ (where $\tau_i = \pm 1$) is a sign-change matrix, it acts by replacing the variables x by $\tau_1 x$, y by $\tau_2 y$, and z by $\tau_3 z$. If $r_0 \le j < r_1$, then $gu_{3,j}^{(2d)} = \tau_1\tau_2 u_{3,j}^{(2d)}$ because all monomials in $u_{i,j}^{(2d)}$ have odd degree in x and y and even degree in z. By symmetry, we have $gu_{1,j}^{(2d)} = \tau_2\tau_3 u_{1,j}^{(2d)}$ and $gu_{2,j}^{(2d)} = \tau_1\tau_3 u_{2,j}^{(2d)}$. For $r_1 \le j < r$, we have $gu_{i,j}^{(2d)} = u_{i,j}^{(2d)}$, since all monomials occurring in $u_{i,j}^{(2d)}$ have even degree in each variable. In the same way, $gu_\infty^{(2d)} = u_\infty^{(2d)}$. Hence, the claim for the action of sign-change matrices is true if we define $\xi(j) := 1$ for $r_0 \le j < r_1$ and $\xi(j) := 0$ for $r_1 \le j < r$.

We now turn to the action of permutation matrices. Note that all permutation matrices can be written as a successive product of

$$g_0 := \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \in B_3 \quad \text{and} \quad g_1 := \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in B_3,$$

so it is enough to show the claim for g_0 and g_1. Denote the permutations of $\{1, 2, 3\}$ corresponding to g_0 and g_1 by σ_0 and σ_1, respectively. Note that $\operatorname{sgn}(\sigma_0) = 1$ and $\operatorname{sgn}(\sigma_1) = -1$.

We have $g_0 u_{i,j}^{(2d)} = u_{\sigma(i),j}^{(2d)}$ for all $j \ge r_0$ by the construction given in Step 2. The element g_1 acts by interchanging the variables x and y in an expression $u_{i,j}^{(2d)}$. The expressions for $u_{3,j}^{(2d)}$ specified in Step 3 were carefully chosen such that we have

$$g_1 u_{3,j}^{(2d)} = (-1)^{j-r_0+d} \cdot u_{3,j}^{(2d)}.$$

This confirms with the claim if we define

$$\xi(j) := \begin{cases} 1 & \text{if } r_0 \leq j < r_1,\ j - r_0 + d \text{ even or } r_1 \leq j < r,\ j - r_1 + d \text{ odd} \\ 0 & \text{otherwise.} \end{cases}$$

That this extends to the action of any permutation matrix on any basis element follows from $u_{1,j} = g_0 u_{3,j}$ and $u_{2,j} = g_0 u_{3,j}$.

This concludes Step 5 and ends the proof. □

Remark 5.15. In the proof we constructed a convenient basis for Λ_{2d} mostly by constructing a convenient basis for the space $\mathcal{H}_{2d}$ of harmonic functions (with B_3-symmetries as described). To be precise, the basis elements $u_{i,j}^{(2d)}$ for $1 \leq i \leq 3$, $r_0 \leq j < r_2$ are all contained in $\mathcal{H}_{2d}$ and, if $d \equiv 2 \pmod 3$, they form a basis of $\mathcal{H}_{2d}$ (by Steps 3 and 4 in the proof). If $d \equiv 0 \pmod 3$, these $u_{i,j}^{(2d)}$ together with $u_\infty^{(2d)}$ form a basis of $\mathcal{H}_{2d}$ (by Step 4).

In the case $d \equiv 1 \pmod 3$, the elements $u_{i,j}^{(2d)}$ for $1 \leq i \leq 3$, $r_0 \leq j < r_2$, together with

$$\tilde{u}_{i,r_2} := u_{i,r_2}^{(2d)} - Q u_\infty^{(2d-2)} \in \mathcal{H}_{2d}\ \forall i \in \{1,2,3\}$$

form a linear *generating set* for $\mathcal{H}_{2d}$. It is not a basis of $\mathcal{H}_{2d}$, since they satisfy the linear dependence

$$\tilde{u}_{1,r_2} + \tilde{u}_{2,r_2} + \tilde{u}_{3,r_2} = 0.$$

In fact, because of the cardinality of this generating set is $\dim \mathcal{H}_{2d} + 1$, this is the only linear dependence relation, and we could extract a basis for $\mathcal{H}_{2d}$ by removing one of the elements $\tilde{u}_{1,r_2}, \tilde{u}_{2,r_2}, \tilde{u}_{3,r_2}$ of our generating set. (However, note that such a removal destroys some symmetry and may make the action of B_3 on $\mathcal{H}_{2d}$ harder to describe.)

CHAPTER 6

Solving the main algorithmic challenges

In Chapters 4 and 5, we have constructed a set of generating rational invariants $\tilde{p}_1, \dots, \tilde{p}_m \in K(V_{2d})^{O(n)}$ for three cases: $d = 1$ and n arbitrary (Section 3.2), $d \geq 2$ and $n = 2$ (Chapter 4), $d \geq 2$ and $n = 3$ (Chapter 5). The invariants might have been indexed differently before, but for convenience we may now assume throughout this chapter that they are numbered from 1 to m. Observe that in all three cases, the number of generating rational invariants m coincides with the lower bound from Theorem 2.15.

$$m = \dim V_{2d} - \dim O(n) = \binom{2d+n-1}{n-1} - \binom{n}{2}.$$

Recall that the construction of the invariants was slightly indirect: Apart from the case $n = 2$, we did not give closed formulas for the invariants $\tilde{p}_i \in K(V_{2d})^{O(n)}$. Instead, we only described explicit formulas for the restriction $p_i := \tilde{p}_i|_{\Lambda_{2d}} \in K(\Lambda_{2d})^{B_n}$ of $\tilde{p}_i \colon V_{2d} \dashrightarrow \mathbb{R}$ to the subspace $\Lambda_{2d} \subset V_{2d}$ defined in Section 3.3. We know by Theorem 3.2 that from a theoretical standpoint, the invariants $\tilde{p}_i \in K(V_{2d})^{O(n)}$ are uniquely characterized by their restrictions $p_i \in K(\Lambda_{2d})^{B_n}$. We will see that this remains true when passing to practical considerations.

In this chapter, we turn to the main algorithmic challenges formulated in Section 2.4. We describe algorithmic solutions, which only rely on information about the restricted invariants $p_i := \tilde{p}_i|_{\Lambda_{2d}} \in K(\Lambda_{2d})^{B_n}$.

6.1. The Evaluation Problem

After we determined a set of generating rational invariants $\tilde{p}_1, \dots, \tilde{p}_m \in K(V_{2d})^{O(n)}$, the most basic algorithmic question is: How can we evaluate $\tilde{p}_1(v), \dots, \tilde{p}_m(v)$ for a given point $v \in V_{2d}$?

By construction of the invariants, we know explicitly the restrictions $p_i := \tilde{p}_i|_{\Lambda_{2d}} \colon \Lambda_{2d} \dashrightarrow \mathbb{R}$, which allow us to compute $\tilde{p}_i(w) = p_i(w) \in \mathbb{R}$ for all $w \in \Lambda_{2d}$. If we want to evaluate $p_i(v)$ for some $v \in V_{2d}$, we observe that $\tilde{p}_i(gv) = \tilde{p}_i(v)$ for all $g \in O(n)$ (because $\tilde{p}_i \in K(V_{2d})^{O(n)}$). By Proposition 3.28, we know that for general $v \in V_{2d}$ there always exists an orthogonal transformation $g \in O(n)$ such that $gv \in \Lambda_{2d}$. For such a $g \in O(n)$, we may then compute

$$\tilde{p}_i(v) = \tilde{p}_i(gv) = p_i(gv)$$

(compare also Remark 3.3).

Recalling the definition of Λ_{2d}, this idea leads to Algorithm 1.

```
  Input  : $v \in V_{2d} = k[x_1, \ldots, x_n]_{2d}$, $d \geq 1$
  Output: $(\tilde{p}_1(v), \ldots, \tilde{p}_m(v)) \in \mathbb{R}^m$
1 Compute $v' \in V_2$ in the Harmonic Decomposition
      $v = h_d + Qh_{2d-2} + Q^2 h_{2d-4} + \ldots + Q^{d-2} h_4 + Q^{d-1} v'$
    (with $h_{2k} \in \mathcal{H}_{2k}$).
2 Let $M \in \mathbb{R}^{n \times n}$ be the Gramian matrix of $v' \in V_2$.
3 Determine $g \in O(n)$ such that the matrix product $gMg^T$ is
    diagonal:
      $gMg^T = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$    for some $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$.
4 If $\lambda_i = \lambda_j$ for some $i \neq j$, output "undefined at $v$" and stop.
5 Compute $w = gv \in \Lambda_{2d}$.
6 Compute and output the values $p_i(w)$ for $i = 1, \ldots, m$.
```

Algorithm 1: Evaluation Algorithm

In the following, we will comment on the validity and on the computational realization of the various steps of Algorithm 1.

First, we convince ourselves that the formulation in Algorithm 1 corresponds to the idea described above of evaluating $\tilde{p}_i(v) = p_i(gv)$ where $g \in O(n)$ is some orthogonal transformation such that $gv \in \Lambda_{2d}$. Recall that if

$$v = h_d + Qh_{2d-2} + Q^2 h_{2d-4} + \ldots + Q^{d-2} h_4 + Q^{d-1} v'$$

is the Harmonic Decomposition of v computed in Step 1, then the Harmonic Decomposition of gv is given as

$$gv = gh_d + Q(gh_{2d-2}) + Q^2(gh_{2d-4}) + \ldots + Q^{d-2}(gh_4) + Q^{d-1}(gv')$$

by Proposition 3.22. Then the definition of Λ_{2d} gives: gv is contained in Λ_{2d} if and only if $gv' \in V_2$ lies in Λ_2, i.e. the Gramian matrix of gv' is diagonal. By Proposition 3.7, the Gramian matrix of gv' is precisely gMg^T (if M is the Gramian matrix of $v' \in V_2$).

It remains to make sense of Step 4 in Algorithm 1. Recall Remark 3.5: Even though the restricted invariants $p_i \in K(\Lambda_{2d})^{B_n}$ are polynomial invariants, the corresponding invariants $\tilde{p}_i \in K(V_{2d})^{O(n)}$ are rational expression[1] which are undefined wherever their denominator vanishes. In fact, going back to the proofs of Propositions 3.28 and 3.9, we see that the rational function $\tilde{p}_i \colon V_{2d} \dashrightarrow \mathbb{R}$ which we obtain from $p_i \in K(\Lambda_{2d})^{B_n}$ is only defined at those points $v \in V_{2d}$ whose quadratic part $v' \in V_2$ (in the Harmonic Decomposition) has a Gramian matrix without repeated eigenvalues.[2] This precisely corresponds to Step 4.

Computational realization of Step 1: Note that for $2d = 2$ we simply have $v' = v$ by definition, so we may consider the case $2d \geq 4$. First, we consider the case $n = 2$.

Recall the basis $u_i^{(2d)}$ $(0 \leq i \leq 2d)$ of V_{2d} from Proposition 4.4. If we write an element $v \in V_{2d}$ as $v = \sum_{i=0}^{2d} \alpha_i u_i^{(2d)}$, then in the Harmonic Decomposition we have $h_{2k} = \alpha_{2k} u_{2k} + \alpha_{2k-1} u_{2k-1}$ with u_i defined as in Proposition 4.2. Therefore, the quadratic part $v' \in V_2$ we are interested in is given as

$$v' = \alpha_2 u_2 + \alpha_1 u_1 + \alpha_0 Q u_0 = (\alpha_0 + \alpha_2)x^2 + 2\alpha_1 xy + (\alpha_0 - \alpha_2)y^2.$$

The element $v \in V_{2d}$ may not be given in the form $v = \sum_{i=0}^{d} \alpha_i u_i^{(2d)}$, but as $v = \sum_{i=0}^{d} a_i x^{d-i} y^i$. These two different ways of writing elements in V_{2d} just correspond to two different choices of bases for the $2d+1$-dimensional vector space V_{2d} (namely $(u_i^{(2d)})_{i=0}^{2d}$ and $(x^{2d-i}y^i)_{i=0}^{2d}$), so converting between the two notions just corresponds to applying a linear change of basis. The base change matrix for passing from $(\alpha_i)_{i=0}^{2d}$ to $(a_i)_{i=0}^{2d}$ is the $(2d+1) \times (2d+1)$-matrix whose (i,j)-th entry (for $0 \leq i, j \leq 2d$) is the coefficient of $x^{2d-j}y^j$ in the expression $u_i^{(2d)}$. This matrix and its inverse (needed for the reverse conversion) can for fixed d already be computed in a preprocessing step. Alternatively, a conversion without matrix inversion can be performed by exploiting the fact that the basis $u_i^{(2d)}$ come from the orthogonal bases (u_{2d-1}, u_{2d}) of $\mathcal{H}_{2d}$ from Proposition 4.2.

The case $n = 3$ equally just amounts to a change of basis: Note here that the basis $u_{i,j}^{(2d)}$ for $1 \leq i \leq 3, 0 \leq j \leq r$ (and possibly $u_\infty^{(2d)}$) of Λ_{2d} extends to a basis of V_{2d} by adding

$$u_{1,-1}^{(2d)} := Q^{d-1} \cdot yz,\ u_{2,-1}^{(2d)} := Q^{d-1} \cdot xz,\ u_{3,-1}^{(2d)} := Q^{d-1} \cdot xy.$$

Note that then for $v = \sum_{i=1}^{3} \sum_{j=-1}^{r} \alpha_{i,j} u_{i,j}^{(2d)}$ $[+\alpha_\infty u_\infty^{(2d)}]$ the quadratic part $v' \in V_2$ of the Harmonic Decomposition is

$$v' = \alpha_{1,3}x^2 + \alpha_{2,3}y^2 + \alpha_{3,3}z^2 + \alpha_{1,-1}yz + \alpha_{2,-1}xz + \alpha_{3,-1}xy.$$

[1] if we actually wrote them out explicitly as closed formulas – which we do not attempt because the resulting expressions would be huge

[2] Leaving out Step 4, Algorithm 1 would still output a value for the non-defined cases, but that value would depend on the choice of g in Step 3.

Converting a description $v = \sum_{i+j+k=2d} a_{i,j,k} x^i y^j z^k \in V_{2d}$ into $v = \sum_{i=1}^{3} \sum_{j=-1}^{r} \alpha_{i,j} u_{i,j}^{(2d)}$ $[+\alpha_\infty u_\infty^{(2d)}]$ can as above be achieved by a linear change of basis.

Computational realization of Step 2: The Gramian matrix M can immediately be read off the quadratic form $v' \in V_2$ by its definition.

Computational realization of Step 3: This problem is known as computing the *eigendecomposition* of the symmetric matrix M and is equivalent to finding the eigenvalues and eigenvectors of M. *Exact (symbolic)* algorithmic solutions to this problem would in particular compute the eigenvalues of M explicitly, which is possible for $n = 2$ (i.e. M is a 2×2-matrix), but would involve introducing square roots (symbolically). For $n = 3$ such an exact is already very undesirable, even though it would in principle be possible by introducing (nested) square roots and cubic roots with Cardano's formulas for solving cubic equations (but such symbolic expressions are hard to work with – for example when deciding equality of two expressions).

However, there are well-established numerical methods for computing the eigendecomposition of a symmetric matrix – with the additional benefit that the numerical stability of these methods is well-studied. One example is the *QR algorithm* (see e.g. [**GVL13**, Chapter 8]) which is based on iterated QR decompositions of matrices.

Computational realization of Step 5: This is straightforward by the definition of the action of $g = (g_{ij}) \in O(n)$: Applying the substitutions

$$x_k \mapsto g_{k1}x_1 + g_{k2}x_2 + \ldots + g_{kn}x_n$$

to $v \in V_{2d} = \mathbb{R}[x_1, \ldots, x_n]_{2d}$ and expanding the resulting expression gives $w = gv \in \Lambda_{2d}$. This expansion may also be precomputed symbolically for fixed d such that it is only necessary to evaluate with the entries g_{ij}.

Computational realization of Step 6: We express $w \in \Lambda_{2d}$ as $w = \sum_{i \neq 1} \alpha_i u_i^{(2d)}$ (for $n = 2$) resp. $w = \sum_{i,j} \alpha_{i,j} u_{i,j}^{(2d)}$ $[+\alpha_\infty u_\infty^{(2d)}]$ (for $n = 3$) according to Propositions 4.4, 5.9 and 5.10. Converting w into this expression corresponds to a linear change of basis as above. Then we evaluate the invariants $p_0, p_2, p_3, \ldots, p_{2d}$ (for $d = 2$) resp. $p_{i,j}$ and p_∞ (for $n = 3$) with their expressions specified in Theorems 4.7 and 5.11.

6.2. The Reconstruction Problem

In Section 6.1, we saw how to numerically compute $(\tilde{p}_1(v), \ldots, \tilde{p}_m(v)) \in \mathbb{R}^m$ for a general point $v \in V_{2d}$. In this section, we consider the inverse algorithmic problem: Given an m-tuple $(\mu_1, \ldots, \mu_m) \in \mathbb{R}^m$, compute $v \in V_{2d}$ such that $\tilde{p}_i(v) = \mu_i$ for all i. This may not be possible for all $(\mu_1, \ldots \mu_m) \in \mathbb{R}^m$, so we are also interested in the following question:

For which m-tuples $(\mu_1, \dots \mu_m) \in \mathbb{R}^m$ does there exist a $v \in V_{2d}$ such that $\tilde{p}_i(v) = \mu_i$ for all i?

Note that the reconstructed $v \in V_{2d}$ is of course not uniquely determined, since for any orthogonally equivalent $w \in V_{2d}$ (i.e. $w = gv$ for some $g \in O(n)$), the invariants $\tilde{p}_i \in K(V_{2d})^{O(n)}$ take the same values for w as for v. Theorem 2.14 implies that typically the reconstructed v is unique up to orthogonal transformations, i.e. any different reconstructed $w \in V_{2d}$ is orthogonally equivalent to v.

Recall that for any $v \in V_{2d}$ there exists $g \in O(n)$ such that $w := gv \in \Lambda_{2d}$. Then

$$\tilde{p}_i(v) = \tilde{p}_i(gv) = p_i(w) \ \forall i \in \{1, \dots, m\}.$$

In particular, we can always choose to reconstruct an element $w \in \Lambda_{2d}$. Since we know explicit formulas for the restricted invariants $p_i := \tilde{p}_i|_{\Lambda_{2d}} \in K(\Lambda_{2d})^{B_n}$, this corresponds to solving a system of equations given by $p_i(w) = \mu_i \ \forall i \in \{1, \dots, m\}$.

We will now treat separately the three cases in which we constructed a set of generating invariants: $d = 1$ and n arbitrary, $d \geq 2$ and $n = 2$, and the case $d \geq 2$ and $n = 3$.

6.2.1. The case of quadratic forms ($2d = 2$).

In Theorem 3.12, we saw that

$$p_k\left(\sum_{i=1}^n \lambda_i x_i^2\right) := \lambda_1^k + \ldots + \lambda_n^k$$

for $1 \leq k \leq n$ form a set of generating rational invariants for the action of B_n on Λ_2. Then the Reconstruction Problem corresponds to solving the system of polynomial equations

$$\lambda_1^k + \ldots + \lambda_n^k = \mu_k \ \forall k \in \{1, \dots, n\}.$$

for $\lambda_1, \dots, \lambda_n$ if possible (where $\mu_1, \dots, \mu_n \in \mathbb{R}$ are given scalars). This particular system of equations is easy to solve: Its resolution is given by the following result:

Proposition 6.1 (Newton's identities). *Let $\lambda_1, \dots, \lambda_n \in \mathbb{C}$ and let $\mu_k := \sum_{i=1}^n \lambda_i^k$ for $k \in \{1, \dots, n\}$. Then $\lambda_1, \dots, \lambda_n$ are the zeroes (with multiplicities) of the degree n polynomial*

$$a_0T^n + a_1T^{n-1} + \ldots + a_{n-1}T + a_n \in \mathbb{C}[T],$$

where $a_0, a_1, \dots, a_n \in \mathbb{C}$ are recursively given as

$$\begin{aligned} a_0 &:= 1, \\ a_k &:= -\frac{1}{k}\sum_{i=1}^k a_{k-i}\mu_i. \end{aligned}$$

Proof. This fact is known under the name *Newton's identities.* Its proof is straightforward: Let

$$f(T) = a_0T^n + a_1T^{n-1} + \ldots + a_{n-1}T + a_n \in \mathbb{C}[T]$$

is the normed polynomial of degree n with zeroes $\lambda_1, \ldots, \lambda_n$ (counted with multiplicities), i.e. $a_0 = 1$ and

$$a_0\lambda_i^n + a_1\lambda_i^{n-1} + \ldots + a_{n-1}\lambda_i + a_n = 0 \ \forall i \in \{1, \ldots, n\}.$$

Summing these equations over all $i \in \{1, \ldots, n\}$ gives

$$a_0\mu_n + a_1\mu_{n-1} + \ldots + a_{n-1}\mu_1 + a_n = 0,$$

showing the recursion for a_k. □

This leads to Algorithm 2.

```
    Input  : $(\mu_1, \ldots, \mu_n) \in \mathbb{R}^n$
    Output: A quadratic form $v \in V_2$ such that $\tilde{p}_k(v) = \mu_k$ for all
            $1 \leq k \leq n$ if possible

 1  $a_0 := 1$
 2  for $k = 1$ to $n$ do
 3      $a_k := -\frac{1}{k}\sum_{i=1}^{k} a_{k-i}\mu_i$
 4  end
 5  Determine $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ as the zeroes (with multiplicities) of
      the polynomial $T^n + a_1T^{n-1} + \ldots + a_{n-1}T + a_n \in \mathbb{R}[T]$
 6  if $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$ then
 7      Output the quadratic form $v := \sum_{i=1}^{n} \lambda_i x_i^2 \in \Lambda_2$.
 8  else
 9      Output "$(\mu_1, \ldots, \mu_n)$ has no reconstruction in $V_2$".
10  end
```

Algorithm 2: Reconstructing a representative in the case $d = 1$.

For Step 5, any numerical root-finding algorithm (over $\mathbb{C}$) for polynomials may be used.

6.2.2. The case of binary forms ($n = 2$, $2d \geq 4$). In Theorem 4.7, we saw that

$$p_k\left(\sum_{i\neq 1} \alpha_i u_i^{(2d)}\right) := \begin{cases} \alpha_k & \text{if } k \equiv 0 \pmod 4, \\ \alpha_2\alpha_3\alpha_k & \text{if } k \equiv 1 \pmod 4, \\ \alpha_2\alpha_k & \text{if } k \equiv 2 \pmod 4, \\ \alpha_3\alpha_k & \text{if } k \equiv 3 \pmod 4 \end{cases}$$

for $k \in \{0, 2, 3, \ldots, 2d\}$ form a set of generating rational invariants for $K(\Lambda_{2d})^{B_2}$. Solving the resulting system of equations for the Reconstruction Problem is straightforward and leads to Algorithm 3.

```
  Input  : $(\mu_0, \mu_2, \mu_3 \dots, \mu_{2d}) \in \mathbb{R}^d$
  Output: A binary form $v \in V_{2d}$ such that $\tilde{p}_k(v) = \mu_k$ for all
          $k \in \{0, 2, 3, \dots, 2d\}$ if possible
1 if $\mu_2 \leq 0$ or $\mu_3 \leq 0$ then
2     Output "$(\mu_1, \dots, \mu_n)$ has no unambiguous reconstruction in
      $V_{2d}$".
3 else
4     $\alpha_2 := \sqrt{\mu_2}$ and $\alpha_3 := \sqrt{\mu_3}$.
5     for $k = 0, 4, 5, \dots, 2d$ do
6         $\alpha_k := \begin{cases} \mu_k & \text{if } k \equiv 0 \pmod 4, \\ \mu_k/(\alpha_2\alpha_3) & \text{if } k \equiv 1 \pmod 4, \\ \mu_k/\alpha_2 & \text{if } k \equiv 2 \pmod 4, \\ \mu_k/\alpha_3 & \text{if } k \equiv 3 \pmod 4) \end{cases}$
7     end
8     Output the binary form $v := \sum_{i \neq 1} \alpha_i u_i^{(2d)} \in \Lambda_{2d}$.
9 end
```

Algorithm 3: Reconstruction in the case $n = 2$, $d \geq 2$.

The validity of Algorithm 3 is immediate from the formulas of the invariants $p_k \in K(\Lambda_{2d})^{B_2}$ and we only need to comment on Step 2. Note that $\mu_2 = \alpha_2^2$ and $\mu_3 = \alpha_3^2$ imply that a reconstruction can only be possible if $\mu_2, \mu_3 \geq 0$. Furthermore, it is not hard to see that whenever $\mu_2 = 0$ or $\mu_3 = 0$ there either exists no reconstruction or there are infinitely many reconstructions $v \in \Lambda_{2d}$ which cannot all be orthogonally equivalent.

For example, for $\mu_2 = \mu_3 = 0$, the system of equations has only a solution if $\mu_k = 0$ for all k not divisible by 4, and there are infinitely many solutions, given by $\alpha_2 = \alpha_3 = 0$, $\alpha_k = \mu_k$ if k is a multiple of 4, and all remaining $\alpha_k \in \mathbb{R}$ can be chosen arbitrarily. These solutions are not all orthogonally equivalent.

6.2.3. The case of ternary forms ($n = 3$, $2d \geq 4$). In Theorems 5.11 and 5.12, we constructed invariants $p_{i,j} \in K(\Lambda_{2d})^{B_3}$ for $1 \leq i \leq 3$ and $0 \leq j < r$ (plus an invariant p_∞ if d is a multiple of 3).

The crucial part in the resolution of the system of equations for the Reconstruction problem lies solving for $\alpha_{1,0}, \alpha_{2,0}, \alpha_{3,0}$ the following equations, arising from the invariants $p_{1,0}, p_{2,0}, p_{3,0}$. Similar to Proposition 6.1 we easily see:

Proposition 6.2. *Let $\mu_{1,0}, \mu_{2,0}, \mu_{3,0} \in \mathbb{C}$. If $\alpha_{1,0}, \alpha_{2,0}, \alpha_{3,0} \in \mathbb{C}$ are a solution of the system*

$$\begin{aligned} \alpha_{1,0}^2 + \alpha_{2,0}^2 + \alpha_{3,0}^2 &= \mu_{1,0}, \\ \alpha_{1,0}\alpha_{2,0}\alpha_{3,0} &= \mu_{2,0}, \\ \alpha_{1,0}^4 + \alpha_{2,0}^4 + \alpha_{3,0}^4 &= \mu_{3,0}, \end{aligned}$$

then the squares $\alpha_{1,0}^2, \alpha_{2,0}^2, \alpha_{3,0}^2 \in \mathbb{C}$ are the zeroes (with multiplicities) of the cubic polynomial

$$T^3 - \mu_{1,0}T^2 + \frac{\mu_{1,0}^2 - \mu_{3,0}}{2}T - \mu_{2,0}^2 \in \mathbb{C}[T].$$

Proof. Let $f \in \mathbb{C}[T]$ be the polynomial whose zeroes (with multiplicities) are $\alpha_{1,0}^2, \alpha_{2,0}^2, \alpha_{3,0}^2$. Then

$$\begin{aligned} f(T) &= (T - \alpha_{1,0}^2)(T - \alpha_{2,0}^2)(T - \alpha_{3,0}^2) \\ &= T^3 - (\alpha_{1,0}^2 + \alpha_{2,0}^2 + \alpha_{3,0}^2)T^2 \\ &\qquad + (\alpha_{1,0}^2\alpha_{2,0}^2 + \alpha_{2,0}^2\alpha_{3,0}^2 + \alpha_{3,0}^2\alpha_{1,0}^2)T - \alpha_{1,0}^2\alpha_{2,0}^2\alpha_{3,0}^2 \\ &= T^3 - \mu_{1,0}T^2 + \frac{\mu_{1,0}^2 - \mu_{3,0}}{2}T - \mu_{2,0}^2. \end{aligned}$$

□

To answer the question when such a system of equations has real solutions, we use:

Proposition 6.3. *A cubic polynomial $f(T) = T^3 - aT^2 + bT - c \in \mathbb{R}[T]$ has three distinct positive real solutions if and only if*

$$a, b, c > 0 \quad \text{and} \quad a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc > 0.$$

Proof. The expression $a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc$ is the *discriminant* of the cubic polynomial f, which has the property that it is positive if and only if f has three distinct real solutions. By Descartes' rule of signs, f has no negative solutions if and only if the signs of the coefficients of f alternate, i.e. $a, b, c > 0$. □

Combining those two results, we obtain Algorithm 4.

For Step 14 in Algorithm 4, it should be observed that an unambiguous reconstruction requires $\alpha_{1,0}^2, \alpha_{2,0}^2, \alpha_{3,0}^2$ to be distinct and non-zero. Then the validity follows from the results given above.

```
Input  : $\mu_{i,j} \in \mathbb{R}$ for $1 \le i \le 3, 0 \le j < r$ [plus $\mu_\infty \in \mathbb{R}$]
Output: A ternary form $v \in V_{2d}$ such that $\tilde{p}_{i,j}(v) = \mu_{i,j}$ for all
        $i, j$ [and $p_\infty = \mu_\infty$] if possible
if $d$ is a multiple of 6 then
    $\alpha_\infty := \mu_\infty$
end
$a := \mu_{1,0}$, $b := \frac{\mu_{1,0}^2 - \mu_{3,0}}{2}$, $c := \mu_{2,0}^2$
if $a, b, c > 0$ and $a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc > 0$ then
    Compute the (distinct) zeroes $t_1, t_2, t_3 > 0$ of the polynomial
      $T^3 - aT^2 + bT - c \in \mathbb{R}[T]$.
    $\alpha_{1,0} := \pm\sqrt{t_1}$, $\alpha_{2,0} := \pm\sqrt{t_2}$, $\alpha_{3,0} := \pm\sqrt{t_3}$, where we choose
      signs such that $\alpha_{1,0}\alpha_{2,0}\alpha_{3,0} = \mu_{2,0}$.
    Calculate the matrix product
      $A := \begin{pmatrix} 1 & 1 & 1 \\ t_1 & t_2 & t_3 \\ t_1^2 & t_2^2 & t_3^2 \end{pmatrix}^{-1} \cdot \begin{pmatrix} \mu_{1,1} & \dots & \mu_{1,r-1} \\ \mu_{2,1} & \dots & \mu_{2,r-1} \\ \mu_{3,1} & \dots & \mu_{3,r-1} \end{pmatrix}$.
    for $1 \le i \le 3, 1 \le j < r$ do
        $\alpha_{i,j} = \frac{A_{i,j}}{\alpha_{i,0}^{\xi(j)} \cdot ((t_1 - t_2)(t_2 - t_3)(t_3 - t_1))^{\zeta(j)}}$.
    end
    Output the ternary form $v := \sum_{i,j} \alpha_{i,j} u_{i,j}^{(2d)}$ [$+\alpha_\infty u_\infty^{(2d)}$] $\in \Lambda_{2d}$.
else
    Output "The values $\mu_{i,j}$ allow no unambiguous
      reconstruction in $V_{2d}$".
end
```

Algorithm 4: Reconstruction in the case $n = 2$, $d \geq 2$.

6.3. The Rewriting Problem

In this section, we want to briefly sketch how the Rewriting Problem specified in Section 2.4 can be addressed.

Since the constructed rational invariants $\tilde{p}_1, \dots, \tilde{p}_m \in K(V_{2d})^{O(n)}$ form a set of generating rational invariants, it must be possible to express any other rational invariant $q \in K(V_{2d})^{O(n)}$ as a rational combination of $\tilde{p}_1, \dots, \tilde{p}_m$, i.e. there must exist a rational expression in m variables $r(T_1, \dots, T_m) \in \mathbb{R}(T_1, \dots, T_m)$ such that

$$q = r(\tilde{p}_1, \dots, \tilde{p}_m).$$

Our aim is: Given $q \in K(V_{2d})^{O(n)}$, find such an $r(T_1, \dots, T_m) \in \mathbb{R}(T_1, \dots, T_m)$.

Note that restricting the above equality to the subspace $\Lambda_{2d} \subset V_{2d}$ gives:

$$q|_{\Lambda_{2d}} = r(p_1, \dots, p_m).$$

Hence, to determine the rational expression r, it is sufficient to rewrite $q|_{\Lambda_{2d}} \in K(\Lambda_{2d})^{B_n}$ in terms of the restricted generating rational invariants $p_1, \dots, p_m \in K(\Lambda_{2d})^{B_n}$. In the proofs of Theorems 3.12, 4.7 and 5.11 we showed that $p_1, \dots, p_m \in K(\Lambda_{2d})^{B_n}$ form a generating set of rational invariants by specifying explicitly how any other rational invariant can be expressed in terms of $p_1, \dots, p_m$. The explicit procedures given there can be converted into a rewriting algorithm in a straightforward way.

Conclusion

This thesis has examined the question how to characterize homogeneous polynomials of even degree up to orthogonal transformations, from a viewpoint of Rational Invariant Theory. We have constructed sets of generating rational invariants of minimal cardinality in the cases of dimensions two and three (i.e. polynomials in two or three variables). This construction has been based on theoretical considerations. Instead of specifying full explicit expressions for the invariants, we have employed the *Slice Method* to characterize them by their restriction to a suitable subspace. We have seen how the main algorithmic challenges associated with rational invariants (evaluation, reconstruction and rewriting) can be solved numerically based on the construction, and the computational realization has been discussed.

Acknowledgement

This thesis grew out of an internship at INRIA Méditerranée in France. Special thanks go to Evelyne Hubert for lots of in-depth discussions on and around this research problem. I want to thank Théo Papadopoulo for introducing me to the topic with context from a Neuroimaging perspective. I am grateful for the hospitality and support from INRIA Méditerranée.

Bibliography

[ABW01] S. Axler, P. Bourdon, and R. Wade. *Harmonic Function Theory*. Graduate Texts in Mathematics. Springer, 2001.

[AKO16] N. Auffray, B. Kolev, and M. Olive. A minimal integrity basis for the elasticity tensor. *ArXiv e-prints*, May 2016. `https://arxiv.org/abs/1605.09561`.

[AM69] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[CTS07] Jean-Louis Colliot-Thélène and Jean-Jacques Sansuc. The rationality problem for fields of invariants under linear algebraic groups (with special regards to the Brauer group). In *Algebraic groups and homogeneous spaces*, volume 19 of *Tata Inst. Fund. Res. Stud. Math.*, pages 113–186. Tata Inst. Fund. Res., Mumbai, 2007.

[DK02] Harm Derksen and Gregor Kemper. *Computational invariant theory*. Invariant Theory and Algebraic Transformation Groups, I. Springer-Verlag, Berlin, 2002. Encyclopaedia of Mathematical Sciences, 130.

[GVL13] Gene H. Golub and Charles F. Van Loan. *Matrix computations*. Johns Hopkins Studies in the Mathematical Sciences. Johns Hopkins University Press, Baltimore, MD, fourth edition, 2013.

[GW09] Roe Goodman and Nolan R. Wallach. *Symmetry, representations, and invariants*, volume 255 of *Graduate Texts in Mathematics*. Springer, Dordrecht, 2009.

[Isa09] I. Martin Isaacs. *Algebra: a graduate course*, volume 100 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2009.

[Oli14] Marc Olive. *Géométrie des espaces de tenseurs Une approche effective appliquée à la mécanique des milieux continus*. Phd thesis, AMU, November 2014. `https://hal.archives-ouvertes.fr/tel-01165379`.

[Stu08] Bernd Sturmfels. *Algorithms in invariant theory*. Texts and Monographs in Symbolic Computation. SpringerWienNewYork, Vienna, second edition, 2008.

[VP94] È. B. Vinberg and V. L. Popov. *Invariant theory*, volume 55 of *Encyclopaedia of Mathematical Sciences*. Springer-Verlag, Berlin, 1994. A translation of ıt Algebraic geometry. 4 (Russian), Akad. Nauk SSSR Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., Moscow, 1989, Translation edited by A. N. Parshin and I. R. Shafarevich.