Testing the equivalence of planar curves

Testing the Equivalence of Planar Curves

CIP-DATA LIBRARY TECHNISCHE UNIVERSITEIT EINDHOVEN

Rijnswou, Sander M. van

Testing the equivalence of planar curves / by Sander M. van Rijnswou. –
Eindhoven : Eindhoven University of Technology, 2001.
Proefschrift. – ISBN 90-386-0861-6

NUGI 811
Subject headings : invariant theory / algorithms
2000 Mathematics Subject Classification : 13A50, 15A72, 15–04, 17B45, 68A15

Printed by Universiteitsdrukkerij Technische Universiteit Eindhoven

Testing the Equivalence of Planar Curves

PROEFSCHRIFT

ter verkrijging van de graad van doctor aan de
Technische Universiteit Eindhoven, op gezag van de
Rector Magnificus, prof.dr. M. Rem, voor een
commissie aangewezen door het College voor
Promoties in het openbaar te verdedigen
op woensdag 11 april 2001 om 16.00 uur

door

Sander Matthijs van Rijnswou

geboren te Delft

Dit proefschrift is goedgekeurd door de promotoren:

prof.dr. A.M. Cohen

en

prof.dr. A. Blokhuis

Contents

Contents **v**

Preface **1**

1 Actions, Tensors and Polynomials **3**
1.1 Introduction . . . 3
1.2 Actions . . . 3
1.3 Invariants and Covariants . . . 6
1.4 Orbits . . . 8

2 Lie algebras **11**
2.1 Introduction . . . 11
2.2 Lie Groups and Lie Algebras . . . 11
2.3 Semisimple Lie Algebras . . . 13
2.4 Decomposition of Lie Algebras . . . 14
2.5 Casimir Operator . . . 17
2.6 Applications to Invariant Theory . . . 17
2.7 The Null-Cone . . . 19

3 The Symbolic Method **23**
3.1 Introduction . . . 23
3.2 Brackets . . . 24
3.3 The Umbral Operator . . . 26
3.4 Evaluation of Bracket Monomials . . . 30
3.5 Invariants for Polynomials of Degree 3 . . . 36
3.6 Invariants for Polynomials of Degree 4 . . . 36
3.7 Invariants for Polynomials of Degree 5 . . . 37
3.8 Overview . . . 39
3.9 Can a Standard Tableau Be a 2-Design? . . . 39

4 Cubics **43**
4.1 Introduction . . . 43
4.2 The Hessian Normal Form . . . 43

4.3 Stabilizers of Cubics 46
4.4 Affine and Projective Stabilizers 48
4.5 Cohomology of Cubic Forms 50
4.6 An Example of a Large Galois Group 54

5 Quartics **57**
5.1 Introduction 57
5.2 Determining Equivalence 59
5.3 The Decomposition of $S^4(S^2(X^*))$ 65
5.4 An Example 67

6 Quintics **71**
6.1 Introduction 71
6.2 Constructing the Covariant 72
6.3 Beyond 76

A Maple Implementations **77**

Bibliography **79**

Index **83**

Dankbetuiging **85**

Samenvatting **87**

Curriculum Vitae **89**

Preface

Invariant theory is an old and interesting subject. A lot of its theory dates back to the 19th and early 20th century. Nevertheless it is still an object of research. For example, a complete generating set of the space of invariants is unknown for relatively small examples such as quartic planar curves. Invariants are used in areas ranging from image processing and mathematical morphology to algebraic geometry.

This thesis looks at the action of the group $\mathrm{SL}_3(\mathbb{C})$ on homogeneous forms in three variables (think of planar curves). In particular we are interested in tests that can determine whether two curves are equivalent with respect to $\mathrm{SL}_3(\mathbb{C})$. One way to do so is by using invariants. When two curves have a different value with respect to some invariant then they are not equivalent. Other ways that we explore use combinations of invariants and covariants. The emphasis is mostly on effective methods. As a way to further investigate the practicality of the proposed algorithms, most of them were implemented on a computer.

In Chapter 1 and Chapter 2 an overview is given of the various results and viewpoints needed for the remaining chapters.

Constructing invariants can be done in different ways. One approach is to identify geometrical properties of the curves under consideration that do not change under the action of the group. Once such invariants are known it is possible to produce others using geometrical or algebraic constructions. An alternative approach is the symbolic method. This method, developed in the 19th century by Aronhold, gives a very concise representation of invariants. In Chapter 3 we investigate how many invariants we can find using this method. Attention is given to the efficiency of such a search.

Some of the theory related to the action of $\mathrm{SL}_3(\mathbb{C})$ on cubics is explored in Chapter 4. For cubics we also look at the equivalence problem when the ground field is an extension of $\mathbb{Q}$. Some of the theorems of this chapter are necessary for later chapters.

In Chapter 5 the equivalence problem is considered for quartics. Various invariants are known for this situation, in fact four of them are determined in Chapter 3, but in this chapter a different approach is developed. Suppose two quartics are given. We examine this pair in two phases. First, these quartics are mapped to quadratic forms. Solving the equivalence problem for these quadrics allows one to simplify the original equivalence problem. Secondly, the simplified quartics are mapped to

quartics in only two variables. These ideas result in an algorithm that, given two sufficiently generic quartics, can find an element of $\mathrm{SL}_3(\mathbb{C})$ that maps one of them to the other, or prove that such an element does not exist.

The ideas that work for quartics can be adapted to work for quintics. Suppose two quintics are given. To determine whether they are equivalent, they are mapped to cubics. It is possible to find all the elements of $\mathrm{SL}_3(\mathbb{C})$ that map one quintic to the other once those elements are found for their related cubics. This is the topic or Chapter 6.

Chapter 1

Actions, Tensors and Polynomials

1.1 Introduction

This chapter introduces various concepts we are using in this thesis. We will look at polynomials as symmetric tensors. It connects the subject with Lie theory and it unifies the group action on the various constructions. Next some definitions from invariant theory are given.

1.2 Actions

The notion of an *action* of a group G on a vector space V is made precise in the following definition.

Definition 1 *Let G be a group, K a field and V a vector space over K. An action of G on V, written as $G\colon V$, is a mapping from $G\times V$ to V (we write $(A,f)\mapsto A\cdot f$) satisfying for all $A,B\in G$, for all $f,g\in V$ and for all $\alpha\in K$: $A\cdot(B\cdot f)=(AB)\cdot f$, $A\cdot(\alpha f+g)=\alpha(A\cdot f)+A\cdot g$ and $1\cdot f=f$.*

The ground field K will often be $\mathbb{C}$, but not always. Given an action of a group G on a vector space V one of the central problems is the *equivalence problem*. That is, given two elements f and g in V, can you decide whether there exists an $A\in G$ such that $A\cdot f=g$. Important tools for this problem are invariants and covariants which we will introduce in this chapter.

First we look at a few examples of actions. Assume we are given a group G and an action on a finite dimensional vector space V over the field K. We will describe how from this given action several different actions on related vector spaces are induced. When convenient we let $e_1,e_2,\ldots,e_n$ be a basis for V. Also let $\phi_1,\ldots,\phi_n$ be the corresponding dual basis of V^*; it satisfies $\phi_i(e_j)=\delta_{ij}$.

Note that an action $G\colon V$ is equivalent to a representation of G on V, that is, a homomorphism $G \to \mathrm{GL}(V)$.

1.2.1 Action of G on V^*

Given the action $G\colon V$ what should an action $G\colon V^*$ look like? First of all it should preserve the relation between a basis and its dual basis. In other words for all $A \in G$, $(A \cdot \phi_i)(A \cdot e_j) = \delta_{ij}$. Or without using these coordinates; for all $\phi \in V^*$ and for all $v \in V$ it should satisfy $(A \cdot \phi)(A \cdot v) = \phi(v)$. This equation determines an action $G\colon V^*$ by $(A \cdot \phi)(v) = \phi(A^{-1} \cdot v)$ for $A \in G$, $\phi \in V^*$, $v \in V$. We can see this by substituting $A^{-1}v$ for v.

We have proven that given an action of G on V, there is a unique action of G on V^* that preserves duality. When we represent the elements of $\mathrm{GL}(V)$ as matrices using the basis $e_1, \ldots, e_n$ and we represent the elements of $\mathrm{GL}(V^*)$ as matrices using the basis $\phi_1, \ldots, \phi_n$ then there is a correspondence between matrices representing the same element.

Lemma 1 *Let the group G act on the finite dimensional vector space V. Suppose $A \in \mathrm{GL}(V)$ and $B \in \mathrm{GL}(V^*)$ both correspond to the same element in G. Then $A = (B^{-1})^\top$.*

Proof: Written on the basis just given, the value of the map $u \in V^*$ on the vector $v \in V$ is given by $u^\top v$. Using the correspondence between the representation of G on V and the related representation on V^* we find

$$(Bu)^\top (Av) = u^\top B^\top A v = u^\top v,$$

for all $u \in V^*$ and $v \in V$. It follows that $A = (B^{-1})^\top$. □

1.2.2 Action of G on Tensor Products.

Now we will extend the action of G to tensor products of V. In general if we have an action of G on the vector spaces $V_1, \ldots, V_k$, we define an action of G (called the natural action) on $V_1 \otimes V_2 \otimes \cdots \otimes V_k$. Given $A \in G$ and $v_1 \otimes v_2 \otimes \cdots \otimes v_k \in V_1 \otimes V_2 \otimes \cdots \otimes V_k$, then $A \cdot (v_1 \otimes v_2 \otimes \cdots \otimes v_k) = (A \cdot v_1) \otimes (A \cdot v_2) \otimes \cdots \otimes (A \cdot v_k)$. The action of A on the other elements of $V_1 \otimes V_2 \otimes \cdots \otimes V_k$ follows by linearity.

In particular we get an action of G on $V^{\otimes k}$. We will use the convention that V^0 denotes the ground field K.

1.2.3 Action of G on Quotient Spaces

Let T be a subspace of V. There is a natural mapping from V to the quotient space V/T defined as $x \mapsto x + T$. In this paragraph we denote $x + T$ by $\overline{x}$. We want to define the action of G on V/T as $g \cdot \overline{x} = \overline{g \cdot x}$. This will be a good definition if $G \cdot T \subset T$ which means $G \cdot T = T$.

One special case is worth mentioning. Consider the vector space $V^{\otimes k}$, and let T be the subspace spanned by the vectors $e_{i_1} \otimes e_{i_2} \otimes \cdots \otimes e_{i_k} - e_{i_{\sigma(1)}} \otimes e_{i_{\sigma(2)}} \otimes \cdots \otimes e_{i_{\sigma(k)}}$,

where $i_j \in \{1, \ldots, n\}$ and σ is a permutation of the integers $\{1, \ldots, k\}$. The space T is stable under the action of G. We denote the space $V^{\otimes k}/T$ by $S^k(V)$, that is the k-symmetric tensor power.

We will identify the space $S^k(V^*)$ with the homogeneous polynomials of degree k on V. In general we will write $v \cdot w$ when we mean the class represented by $v \otimes w$, that is $v \cdot w = v \otimes w + T$.

1.2.4 Homogeneous Polynomials

Let V be an n-dimensional vector space. Consider $P = S^k(V^*)$, the k-th symmetric power of its dual. The space V^* is spanned by the coordinate functions x_1, $x_2, \ldots, x_n$. An element of P that is in the same quotient class as $x_{a_1} \otimes x_{a_2} \otimes \cdots \otimes x_{a_k}$ is called a monomial. Given a monomial $x_{a_1} \otimes x_{a_2} \otimes \cdots \otimes x_{a_k}$ in $S^k(V^*)$, the following map determines a mapping from V to V^0:

$$V \to V^0 \colon v \mapsto x_{a_1}(v) x_{a_2}(v) \cdots x_{a_k}(v).$$

This mapping can be uniquely linearly extended to all of $S^k(V^*)$. A mapping that arises in this manner is called a homogeneous polynomial function of degree k. Usually we view the elements of $S^k(V^*)$ as abstract objects that are not to be identified with the mapping that corresponds to them. Indeed, if the underlying field if finite, such an identification is impossible. Sometimes, this identification will be useful however. Accordingly the space $S^k(V^*)$ will sometimes be denoted as $K[V]_k$, when we want to put emphasis on the polynomial interpretation of this space. The action on $S^k(V^*)$ is given by Subsection 1.2.3.

We define the derivative $\frac{\partial}{\partial x_k}$ on $S^m(V^*)$ by requiring

$$\frac{\partial}{\partial x_k} x_i = \begin{cases} 1 & \text{if } i = k, \\ 0 & \text{if } i \neq k, \end{cases}$$

that it is linear, and that it satisfies the product rule: $\frac{\partial}{\partial x_k}(fg) = \left(\frac{\partial}{\partial x_k} f\right) g + f \cdot \left(\frac{\partial}{\partial x_k} g\right)$. The following is a convenient identity linking these partial derivatives to f.

Lemma 2 (Euler) *Let f be a homogeneous polynomial of degree k in the variables $x_1, \ldots, x_n$. The following holds:*

$$x_1 \frac{\partial}{\partial x_1} f + x_2 \frac{\partial}{\partial x_2} f + \cdots + x_n \frac{\partial}{\partial x_n} f = k \cdot f.$$

Proof: Since the derivative is linear we may assume that f is a monomial. Let $f = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$. Then $x_i \frac{\partial}{\partial x_i} f = \alpha_i \cdot f$, note that this is true for all non-negative values of α_i. Since $\sum \alpha_i = k$ the result follows. □

Definition 2 *Let f be a homogeneous polynomial in the variables $x_1, \ldots, x_n$. We say that f is singular when f, $\frac{\partial}{\partial x_1} f, \frac{\partial}{\partial x_2} f, \ldots, \frac{\partial}{\partial x_n} f$ have a non-zero root in common.*

Assuming that the degree k of f is not a multiple of the characteristic of the field K, then we have by Lemma 2, that the derivatives $\frac{\partial}{\partial x_1}f, \frac{\partial}{\partial x_2}f, \ldots, \frac{\partial}{\partial x_n}f$ have a zero in common if and only if $f, \frac{\partial}{\partial x_1}f, \frac{\partial}{\partial x_2}f, \ldots, \frac{\partial}{\partial x_n}f$ have a zero in common.

1.3 Invariants and Covariants

Definition 3 *Let V and W be vector spaces on which a group G acts. A mapping $\phi\colon V \to W$ which respects this action, in the sense that for all $A \in G$ and all $v \in V$ we have $\phi(A \cdot v) = A \cdot \phi(v)$, is said to be G-covariant.*

The word covariant is both used as a noun and as an adjective. So in the previous definition ϕ is a G-covariant and ϕ is a G-covariant mapping. An invariant is a particular kind of covariant:

Definition 4 *Let V be a vector space over the field K. Let G be a group that acts on V. A G-invariant is a mapping $\phi\colon V \to K$ such that for all $A \in G$ and for all $v \in V$ we have $\phi(A \cdot v) = \phi(v)$.*

Note that covariants or invariants do not need to be linear. Invariants obviously are of help in solving the equivalence problem. Suppose we are given f and g and an appropriate invariant ϕ. If $\phi(f) \neq \phi(g)$ then they are not equivalent. Covariants can not be applied as directly as that. But on the other hand since they keep more information about the objects they are potentially more powerful. The following lemma shows how covariants can help in solving the equivalence problem.

Lemma 3 *Let G be a group and let V and W be vector spaces on which G acts. Let $\phi\colon V \to W$ be a G-covariant mapping. Let $f, g \in V$ and put $T = \{A \in G \mid A \cdot f = g\}$ and $U = \{A \in G \mid A \cdot \phi(f) = \phi(g)\}$. Then $T \subset U$.*

Proof: Let $B \in T$ then $B \cdot f = g$ hence, by covariance, $B\phi(f) = \phi(g)$, that is $B \in U$. □

This lemma will be applied in Chapters 5 and 6.

Usually a covariant maps polynomials of a certain degree to polynomials of some other degree, that is, they are mappings $S^d(V^*) \to S^k(V^*)$. Sometimes such maps do not exist but a map like $S^d(V^*) \to S^k(V)$ does exist. As long as such a map respects the action of the group, they are covariants, according to Definition 3. These particular maps are also often called *contravariants*.

Example: Let V be a vector space on which the group G acts. Let $k > 0$ be an integer. Define the mapping $\rho\colon V \to V^{\otimes k}$ by $v \mapsto v \otimes v \otimes \cdots \otimes v$. Let G act on $V^{\otimes k}$ as suggested in Subsection 1.2.2 (this special case is also known as the *diagonal action*). Now we have: $\rho(A \cdot v) = (A \cdot v) \otimes \cdots \otimes (A \cdot v)$ and $A \cdot \rho(v) = A \cdot (v \otimes \cdots \otimes v)$. These two expressions are equal and hence ρ is a covariant. This construction also works when we take quotients of vector spaces. In particular there is a covariant mapping from V to $S^k(V)$.

Example: We will return to this example in Section 1.4. This example will be written out in full to illustrate the actions. Let $X = \mathbb{C}^2$ and let X^* be spanned by the coordinate functions x and y. Let $G = \mathrm{SL}(X)$ act on the space $S^2(X^*)$. We have:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot x = dx - by, \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot y = -cx + ay.$$

Define the function $\phi\colon S^2(X^*) \to \mathbb{C}$ by $\phi(ux^2 + 2vxy + wy^2) = v^2 - uw$.

Theorem 1 *The mapping ϕ is an invariant.*

Proof: Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be an arbitrary element of $\mathrm{SL}(X)$. Then we obtain:

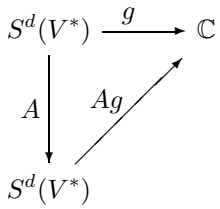
$$\begin{aligned} &\phi(A \cdot (ux^2 + 2vxy + wy^2)) = \\ &\phi(u(dx - by)^2 + 2v(dx - by)(-cx + ay) + w(-cx + ay)^2) = \\ &\phi((-2vdc + ud^2 + wc^2)x^2 + 2(-udb + vbc + vda - wca)xy + \\ &\qquad (ub^2 + wa^2 - 2vba)y^2) = \\ &(ad - bc)^2(v^2 - uw) = (v^2 - uw) = \\ &\phi(ux^2 + 2vxy + wy^2). \end{aligned} \tag{1.1}$$

This shows that ϕ is an invariant. □

A slight modification gives an example of a covariant which is not an invariant. Let $G = \mathrm{GL}(X)$, let G act on $\mathbb{C}$ by $A \cdot x = \det(A)x$. In this setting, the mapping ϕ is a covariant.

1.3.1 Representing Invariants

Let $V = \mathbb{C}^n$. Let $g\colon S^d(V^*) \to \mathbb{C}$ be a homogeneous polynomial, that maps homogeneous polynomials of degree d to $\mathbb{C}$. Let m be the degree of g. Such a function can be seen as a polynomial in a basis for $S^d(V^*)^*$. Since g is of degree m, we can represent it as a point in $S^m(S^d(V^*)^*)$. Let $A \in \mathrm{SL}(V)$. The following diagram commutes, by the construction of Subsection 1.2.1.



In the particular case where g is an invariant, we have $Ag = g$. Hence polynomial invariants, homogeneous of degree m corresponds to fixed points of $S^m(S^d(V^*)^*)$.

The action of $\mathrm{SL}(V)$ on polynomials preserves the degree of all the monomials. Hence, a polynomial invariant of degree m is a linear combination of homogeneous

polynomial invariants of degree m or less. Therefore we will assume without loss of generality that a polynomial invariant of degree m is in fact a homogeneous invariant of degree m.

1.4 Orbits

Definition 5 *Let G be a group that acts on the vector space V. The* orbit *of element $f \in V$ is the set*

$$\{A \cdot f \mid A \in G\}.$$

By definition, an invariant gives the same value for all the elements of an orbit. We illustrate orbits with the following example.

Example: We use essentially the same action as in the example of Section 1.3. Let the ground field K be the finite field with q elements. Assume q is odd. We consider the action $\mathrm{GL}_n(K)\colon S^2(V)$ where V is a vector space of dimension n.

Given a basis $x_1, \ldots x_n$ of V^*, we can link a symmetric matrix M with entries m_{ij} with the binary form $\underline{x}^\top M \underline{x} = \sum m_{ij} x_i x_j$, where $\underline{x} = (x_1, \ldots, x_n)^\top$. The action of A on binary forms corresponds to the action $M \mapsto A^\top M A$ for the matrix interpretation. Note that in this fashion it is immediate that $\det(M)$ is an invariant for the group $\mathrm{SL}(V)$, since $\det(A^\top M A) = \det(A)^2 \det(M)$.

Theorem 2 *Let K be a finite field of odd characteristic. Let $a \in K$ be a non-square. Then a quadratic form in the variables $x_1, \ldots, x_n$ is equivalent under $\mathrm{GL}_n(K)$ to one of the forms: 0, x_1^2, ax_1^2, $x_1^2 + x_2^2$, $x_1^2 + ax_2^2$, …, $x_1^2 + \cdots + x_n^2$, $x_1^2 + \cdots + ax_n^2$.*

Proof: We can use the ordinary algorithm to diagonalize a quadric. This will not work in characteristic 2. After that we can scale any nonzero coefficient to 1 or a particular non-square. Using the matrix

$$\begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix}$$

where $\alpha^2 + \beta^2 = a$ (this equation always has a solution, see next lemma) we can then change the number of coefficients a to 1 or 0. Furthermore rank and determinant are sufficient to see that no two of these forms are mutually equivalent. □

Lemma 4 *Let a be a non-square element in the finite field K of odd order q. The equation $\alpha^2 + \beta^2 = a$ has a solution.*

Proof: First we show that the set $\{x^2 + y^2 \mid x, y \in K\}$ cannot contain only squares. If it would then the squares would form a subfield of order $\frac{q+1}{2}$. But $\frac{q+1}{2}$ is not a divisor of q. So suppose we have $\alpha'^2 + \beta'^2 = a'$, with a' a non-square. Since a/a' is a square we can multiply the equation by it and get the desired solution. □

Proposition 1 *Let K be a field of odd characteristic with q elements. Let $\mathrm{GL}_2(K)$ act naturally on binary quadric. There are five orbits. Table 1.1 gives the size of each orbit along with a representative.*

Representative	Size of Stab	Size of Orbit
0	$\lvert\mathrm{GL}_2(K)\rvert$	1
x_1^2	$2q(q-1)$	$\frac{q^2-1}{2}$
ax_1^2	$2q(q-1)$	$\frac{q^2-1}{2}$
$x_1^2 - x_2^2$	$2(q-1)$	$\frac{q(q^2-1)}{2}$
$x_1^2 - ax_2^2$	$2(q+1)$	$\frac{q(q-1)^2}{2}$

Table 1.1: Orbits of the action of $\mathrm{GL}_2(K)$ on quadrics

Proof: We get the representatives of the orbits form Theorem 2. First note that $\lvert\mathrm{GL}_2(K)\rvert = (q^2-1)(q^2-q) = q(q-1)^2(q+1)$, and that $\lvert S^2(V)\rvert = q^3$. Indeed the sum of the right column of Table 1.1 is q^3. The stabilizers of the first four lines are straightforward to compute and from those the size of the orbits. Of particular interest is the last line of this table. We will show the computations now. Enlarge the field K with the square root of $a = \omega^2$. Now the form splits into the product of two linear forms. Hence the stabilizer has size $2(q^2-1)$. Now we have to count how many of elements of this stabilizer are in the ground field. Permuting x_1 and x_2 is in the stabilizer. We will do one case here. We compute the precise form of the stabilizers and then derive equations that need to be satisfied. Associated to this form is a matrix: set

$$M = \begin{pmatrix} 1 & 0 \\ 0 & -a \end{pmatrix},$$

and let

$$T = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ \frac{-1}{\omega} & \frac{1}{\omega} \end{pmatrix}.$$

Then we have $T^\top M T = \begin{pmatrix} 0 & 1/2 \\ 1/2 & 0 \end{pmatrix}$. That is, the matrix T transforms the form $x_1^2 - ax_2^2$ to x_1x_2. The stabilizer of M can be found by computing, for all $\lambda \in K(\omega)$:

$$T\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}T^{-1} = \frac{1}{2}\begin{pmatrix} \lambda+\lambda^{-1} & (-\lambda+\lambda^{-1})\omega \\ (-\lambda+\lambda^{-1})\omega^{-1} & \lambda+\lambda^{-1} \end{pmatrix}.$$

To restrict the stabilizer over the larger field $K(\omega)$ to the stabilizer over the smaller field K, we need to solve the following equations:

$$\lambda + \lambda^{-1} \in K \tag{1.2}$$

$$(-\lambda + \lambda^{-1})\omega \in K \tag{1.3}$$

Setting $\lambda = \lambda_1 + \omega\lambda_2$ this reduces to $\lambda_1^2 - a\lambda_2^2 = 1$, that is the norm of λ is 1. The $\lambda \in K(\omega)$ that have norm 1 form a subgroup of order $q + 1$. Including the permutation we get a stabilizer of size $2(q + 1)$.

□

Remark: A similar classification can be done for ternary quadrics. A normal form for that case will be used in Chapter 5.

Chapter 2

Lie algebras

2.1 Introduction

In this chapter we will write down a theory that will make it easier to work with a group like SL_n. The defining property of this group, namely that its elements have determinant 1, is a polynomial of degree n. This non-linearity makes it hard to deal with. We will see that there is a certain algebra $\mathfrak{sl}_n$ corresponding to SL_n that satisfies two wishes. On the one hand many of its properties are the same as the properties of SL_n; on the other hand it has a much simpler structure.

The theory of Lie algebras, which allows this fortunate situation, not only applies to SL_n but to a much larger class, the so-called Lie groups. Our main interest lies with the former group though. A lot of this material comes from (Fulton and Harris 1991), but other interesting references are (Jacobson 1979; de Graaf 2000).

2.2 Lie Groups and Lie Algebras

2.2.1 Lie Groups

Definition 6 *A* topological group *G is a group G, whose underlying set is a topological space with respect to which the group operations are continuous.*

Definition 7 *A (complex)* Lie group *G is a topological group whose underlying space is an analytic (complex) manifold on which the group operations are analytic.*

Example: The group of invertible linear transformations of a complex vector space V, that is $\mathrm{GL}(V)$, is a complex Lie group. The manifold structure comes from the complex vector space $\mathrm{End}(V)$. Introducing coordinates for V, the matrix entries are coordinates on $\mathrm{GL}(V)$. Since group multiplication is a polynomial function and the inverse function is a rational function, both are continuous and analytic. Also the closed subgroup $\mathrm{SL}(V) = \{h \in \mathrm{GL}(V) \mid \det(h) = 1\}$ is a Lie group. When the vector space V is n-dimensional and the representation is natural, we will abbreviate

this to GL_n and SL_n.

Since Lie groups are equipped with both a topology and a group multiplication they have a rich structure. A small part of a Lie group determines the whole group. In fact if the group is connected, any neighborhood of the identity generates the whole group.

Proposition 2 *Let G be a connected topological group, and $U \subset G$ any neighborhood of the identity. Then U generates G.*

Proof: Let $\tilde{U} = \langle U \rangle$. We will show that $\tilde{U}$ is both an open and a closed subset of G. Since G is connected and $\tilde{U}$ is not empty this implies that $\tilde{U} = G$.

First we show that $\tilde{U}$ is open. Let $a \in \tilde{U}$, by construction $a \cdot U \subset \tilde{U}$. The set $a \cdot U$ is open since the multiplication of the Lie group is continuous.

Next we show that $\tilde{U}$ is closed. Let $g \notin \tilde{U}$. The set $g \cdot U$ is open. Suppose $g \cdot U \cap \tilde{U} \neq \emptyset$. Then $g \in \tilde{U} \cdot U^{-1} = \tilde{U}$. This is a contradiction. Hence the complement of $\tilde{U}$ is open. □

Example: Both $\mathrm{GL}_n(\mathbb{C})$ and $\mathrm{SL}_n(\mathbb{C})$ are connected.

2.2.2 Lie Algebras

Closely related to Lie groups are so-called *Lie algebras*. We will first give the definition.

Definition 8 *A Lie algebra $\mathfrak{g}$ is a vector space together with a map (the bracket)*

$$[\ ,\ ]\colon \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$$

that satisfies the following identities:

- *The bracket is bilinear,*
- $[a, a] = 0$ *for all* $a \in \mathfrak{g}$,
- $[a, [b, c]] + [b, [c, a]] + [c, [a, b]] = 0$ *for all* $a, b, c \in \mathfrak{g}$.

For each Lie group G a corresponding Lie algebra $\mathfrak{g}$ can be constructed. The vector space for $\mathfrak{g}$ is the tangent space of G at the origin T_eG. The Lie bracket is defined in a few steps. First a Lie group automorphism is given by $\psi_g(h) = ghg^{-1}$. Next we define a function $Ad\colon G \to \mathrm{Aut}(T_eG)$ by $Ad(g) = (d\psi_g)_e$. Differentiation of this function gives a function $ad\colon T_eG \to \mathrm{End}(T_eG)$. Finally the bracket is defined by $[X, Y] = ad(X)(Y)$.

Example: Let $G = \mathrm{GL}_n(\mathbb{C})$. The corresponding Lie algebra $\mathfrak{gl}_n(\mathbb{C})$ is the vector space $T_eG = \mathrm{End}(V)$. The Lie bracket is the commutator $[X, Y] = XY - YX$. In general, for subgroups of the Lie group $\mathrm{GL}_n(\mathbb{C})$ the bracket of the Lie algebra is the commutator. The Lie algebra corresponding to $\mathrm{SL}_n(\mathbb{C})$ is $\mathfrak{sl}_n(\mathbb{C})$, the $n \times n$ matrices with trace zero.

A *representation of a Lie algebra* $\mathfrak{g}$ is a vector space V together with a Lie algebra homomorphism from $\mathfrak{g}$ to $\mathfrak{gl}(V)$.

In general it is easier to work with a Lie algebra than with a Lie group. This is because Lie algebras are linear objects, whereas Lie groups are in general non-linear. Fortunately, the following theorem allows us to do most of our computations in a Lie algebra instead of a Lie group.

Theorem 3 *Let G and H be Lie groups with G simply connected. Let $\mathfrak{g}$ and $\mathfrak{h}$ be the corresponding Lie algebras. There is a bijective correspondence between morphisms of G and H and morphisms of $\mathfrak{g}$ and $\mathfrak{h}$.*

In particular, any subalgebra of a Lie algebra corresponds to a subgroup of the Lie group.

Using the definitions from Chapter 1 and the algorithm for finding the Lie algebra of a Lie group, one can deduce what the action of a Lie algebra should be when we let it act on tensor products or dual spaces. We take from (Fulton and Harris 1991)[pp. 110] the following two constructions. Let V and W be a representation of the Lie algebra $\mathfrak{g}$. Let $e \in \mathfrak{g}$. The action of e on $v \otimes w \in V \otimes W$ is

$$e(v \otimes w) = e(v) \otimes w + v \otimes e(w).$$

If $\rho\colon \mathfrak{g} \to \mathfrak{gl}(V)$ gives a representation of $\mathfrak{g}$ on V, then a corresponding representation ρ^* on V^* can be defined by $(\rho^*(e)\phi)x = \phi(-\rho(e)x)$ for $e \in \mathfrak{g}$, $\phi \in V^*$ and $x \in V$. Choosing coordinates for V and V^* allows us to write $\phi = v^\top$ for some $v \in V$ and $(\rho^*(e)\phi)x = -v^\top \rho(e)x = (-\rho(e)^\top v)^\top x$. Writing the action on V^* as a left action we obtain $-\rho(e)^\top$ for the representation of e.

2.3 Semisimple Lie Algebras

In this section we will introduce a number of concepts that are relevant to Lie algebras. In particular we will introduce the important notion of semisimplicity.

Let $\mathfrak{g}$ be a Lie algebra.

Definition 9 *The lower central series of $\mathfrak{g}$ is defined by the following recurrence relations:*

$$C^1\mathfrak{g} = \mathfrak{g}$$
$$C^n\mathfrak{g} = [\mathfrak{g}, C^{n-1}\mathfrak{g}]$$

Definition 10 *The derived series of $\mathfrak{g}$ is defined by the following recurrence relations:*

$$D^1\mathfrak{g} = \mathfrak{g}$$
$$D^n\mathfrak{g} = [D^{n-1}\mathfrak{g}, D^{n-1}\mathfrak{g}]$$

If A and B are subsets of $\mathfrak{g}$ then $[A, B]$ is taken to mean the subalgebra of $\mathfrak{g}$ spanned by all elements of the form $[a, b]$ with $a \in A$ and $b \in B$.

Definition 11 *A Lie algebra $\mathfrak{g}$ is nilpotent if there is an n such that $C^n\mathfrak{g}$=0.*

For example every abelian Lie algebra is nilpotent since in that case $C^2\mathfrak{g} = [\mathfrak{g}, \mathfrak{g}] = 0$.

Definition 12 *A Lie algebra is solvable if there is an n such that $D^n\mathfrak{g} = 0$.*

Proposition 3 *Every nilpotent Lie algebra is solvable.*

Proof: We will show with induction that $D^n\mathfrak{g} \subset C^n\mathfrak{g}$. For $n = 1$ the proposition follows from the definition. Suppose that for a certain n we have $D^n\mathfrak{g} \subset C^n\mathfrak{g}$. Then $C^{n+1}\mathfrak{g} = [\mathfrak{g}, C^n\mathfrak{g}]$ and $D^{n+1}\mathfrak{g} = [D^n\mathfrak{g}, D^n\mathfrak{g}]$. Since $D^n\mathfrak{g} \subset \mathfrak{g}$ and $D^n\mathfrak{g} \subset C^n\mathfrak{g}$ the proposition is also true for $n + 1$. This completes the induction argument. Since $\mathfrak{g}$ is nilpotent there is an n such that $C^n\mathfrak{g} = 0$ hence also $D^n\mathfrak{g} = 0$. □

There is a notion of ideals for Lie algebras.

Definition 13 *The set $\mathfrak{a} \subset \mathfrak{g}$ is an ideal of $\mathfrak{g}$ if $\mathfrak{a}$ is a Lie subalgebra of $\mathfrak{g}$ and $[\mathfrak{a}, \mathfrak{g}] \subset \mathfrak{a}$.*

Definition 14 *A Lie algebra $\mathfrak{g}$ is* semisimple *if it has no solvable ideals.*

Definition 15 *An element x of a semisimple Lie algebra is called semisimple when* $\operatorname{ad} x$ *is diagonalizable.*

Definition 16 *Let $\mathfrak{a} \subset \mathfrak{g}$ be a subalgebra of the Lie algebra $\mathfrak{g}$. The normalizer of $\mathfrak{a}$ is defined as: $\mathfrak{n}(\mathfrak{a}) = \{x \in \mathfrak{g} \mid [x, \mathfrak{a}] \subset \mathfrak{a}\}$.*

The Lie algebra $\mathfrak{sl}_n(\mathbb{C})$ is simple (does not contain non-trivial ideals and has dimension greater than 1). When a Lie algebra is simple this implies that it is also semisimple. The following is Theorem 9.19 in (Fulton and Harris 1991).

Theorem 4 (Complete Reducibility) *Let V be a representation of the semisimple Lie algebra $\mathfrak{g}$ and suppose $W \subset V$ is a subspace invariant under the action of $\mathfrak{g}$. Then there exists a subspace $W' \subset V$ complementary to W and invariant under $\mathfrak{g}$.*

Remark: The conclusion of Theorem 4 also holds for so-called reductive Lie algebras over $\mathbb{C}$. For example $\mathfrak{gl}_n(\mathbb{C})$ is reductive.

2.4 Decomposition of Lie Algebras

The goal of this section is to give an overview of that part of Lie algebra theory that underlies the remainder of this thesis. Our emphasis will lie mostly on the

algorithmic aspects of the theory. We will follow mainly (Fulton and Harris 1991) and (Jacobson 1979); those are also the prime references for the missing proofs.

Let V be a representation of a semisimple Lie algebra $\mathfrak{g}$. (That is a Lie algebra homomorphism $\mathfrak{g} \to \mathfrak{gl}(V)$.) We write the theory down with respect to this representation. Keep in mind however that for us the prime example of a semisimple Lie algebra is just $\mathfrak{sl}_3(\mathbb{C})$. The running text will therefore be interspersed with an example how this relates to $\mathfrak{sl}_3(\mathbb{C})$.

2.4.1 The Cartan Subalgebra

Definition 17 *Let $\mathfrak{g}$ be a Lie algebra. Let $\mathfrak{h}$ be an abelian subalgebra such that all elements of $\mathfrak{h}$ are semisimple. If moreover $\mathfrak{h}$ is maximal with respect to these properties then $\mathfrak{h}$ is a Cartan subalgebra.*

An alternative but equivalent definition can be found in (Serre 1987). It uses the normalizer.

Definition 18 *A subalgebra $\mathfrak{h}$ of $\mathfrak{g}$ is a Cartan subalgebra if it is nilpotent and $\mathfrak{n}(\mathfrak{h}) = \mathfrak{h}$.*

Every Lie algebra has a Cartan subalgebra (see (Serre 1987) or (Fulton and Harris 1991)). A Cartan subalgebra will often be denoted with the letter $\mathfrak{h}$.

Example: Let the vector space V be $\mathbb{C}^2$. Consider the subalgebra of $\operatorname{End} V$ of all endomorphisms of trace zero. It is isomorphic to $\mathfrak{sl}_2(\mathbb{C})$. Let $\mathfrak{h}$ be the subalgebra of $\mathfrak{sl}_2(\mathbb{C})$ consisting of all the diagonal matrices. This subalgebra is commutative, hence nilpotent. We will prove that it is equal to its normalizer. Let $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ and let $l = \begin{pmatrix} \lambda & 0 \\ 0 & -\lambda \end{pmatrix}$. Then $[A, l] = \lambda \begin{pmatrix} 0 & -2a_{12} \\ 2a_{21} & 0 \end{pmatrix}$. If $\lambda \neq 0$ then this is only diagonal if A is diagonal. Hence $\mathfrak{n}(\mathfrak{h}) = \mathfrak{h}$ and $\mathfrak{h}$ is a Cartan subalgebra. Elements of $\mathfrak{sl}_2(\mathbb{C})$ have trace zero so the algebra $\mathfrak{h}$ is spanned by one element:

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

This approach can also be used to show that in general the subalgebra of diagonal matrices of trace zero is a Cartan subalgebra of $\mathfrak{sl}_n(\mathbb{C})$.

2.4.2 Weights

Let a Cartan subalgebra $\mathfrak{h}$ act on the Lie algebra $\mathfrak{g}$ by the adjoint representation. This action turns out to be diagonalizable and we obtain the decomposition

$$\mathfrak{g} = \mathfrak{h} \oplus (\oplus_\alpha \mathfrak{g}_\alpha).$$

In this decomposition the α are elements of $\mathfrak{h}^*$; these eigenvalues are called *roots*. Let R be the set of all roots. The corresponding subspaces $\mathfrak{g}_\alpha$ are called *root spaces*.

In the same manner, the vector space V decomposes into eigenspaces when $\mathfrak{h}$ acts on it. The subspace $V_\alpha \neq 0$ corresponds to the eigenvalue $\alpha \in \mathfrak{h}^*$, called a *weight* of $\mathfrak{h}$ (with respect to V). We have the following direct sum decomposition:

$$V = \oplus_\alpha V_\alpha.$$

The weight spaces have the property that for any root α and weight β,

$$\mathfrak{g}_\alpha \colon V_\beta \to V_{\beta+\alpha}.$$

Next we will order the roots in R by picking a real, linear functional on $\mathfrak{h}^*$. We can do this in such a way that no weight gets the value zero, nor that two weights in R are equal with respect to this functional. This induces a partition of R in R^+ and R^-, the positive and the negative roots.

Definition 19 *A non-zero vector of V is a* highest weight *if it is an eigenvalue of $\mathfrak{h}$ and it lies in the kernel of $\mathfrak{g}_\alpha$ for all $\alpha \in R^+$.*

Theorem 5 *Let v be a highest weight vector of V. The subspace W of V generated by $\mathfrak{g} \cdot v$ is irreducible.*

The following theorem is Proposition 14.3 in (Fulton and Harris 1991).

Theorem 6 *Let V be a representation of a semisimple Lie algebra $\mathfrak{g}$. Then V contains a highest weight vector v. Moreover if V is an irreducible representation then this vector is unique up to scalar multiplication.*

Example: As noted in a previous example, a Cartan subalgebra $\mathfrak{h}$ of $\mathfrak{g} = \mathfrak{sl}_3(\mathbb{C})$ equals the subalgebra of diagonal matrices of trace zero. There are six root spaces of $\mathfrak{g}$ corresponding to a non-zero root. Each one is one dimensional and spanned by an element $E_{i,j}$. Here $1 \leq i, j \leq 3$, $i \neq j$ and $E_{i,j}$ is a 3×3 matrix that is everywhere zero except in the entry (i, j) which is one.

Example: We will illustrate the theory of this chapter in an example. Let $V = \mathbb{C}^2$ for which we take x, y as a basis. Let the $\mathrm{SL}(V)$ action extend to $S^2(V)$ and to $S^2(S^2(V))$. It is our intention to find an $\mathrm{SL}_2(\mathbb{C})$ invariant subspace of the latter.

First of all we switch to the Lie algebra action of $\mathfrak{sl}_2(\mathbb{C})$. When seen as a vector space $\mathfrak{sl}_2(\mathbb{C})$ is spanned by the following elements.

$$X = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad H = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

The algebra spanned by H is a one dimensional Cartan subalgebra. Highest weight vectors are eigenvalues of H and lie in the kernel of X. Since $x^2 \cdot x^2$ has weight 4, the highest overall weight, it is also a highest weight vector. The second highest weight is 2, but there is no highest weight vector associated to it. The vectors of weight 0 are $\alpha x^2 \cdot y^2 + \beta xy \cdot xy$, parameterized by $\alpha, \beta \in \mathbb{C}$. To see if a highest weight vector lies in that subspace we let X act on it

$$X \cdot (\alpha x^2 \cdot y^2 + \beta xy \cdot xy) = \alpha x^2 \cdot 2xy + \beta 2y^2 \cdot xy.$$

We get a highest weight vector whenever $\alpha = -\beta$; we will use $x^2 \cdot y^2 - xy \cdot xy$. If we let Y act on this vector we get 0. From this we see that it is a one dimensional subspace. By the correspondence between $\mathfrak{sl}_2(\mathbb{C})$ decompositions and $\mathrm{SL}_2(\mathbb{C})$ decompositions (see Theorem 3), we know that it is also a $\mathrm{SL}_2(\mathbb{C})$ invariant element. For example, if we let

$$B = \begin{pmatrix} 1 & 2 \\ 2 & 5 \end{pmatrix}$$

act on it, we obtain:

$$\begin{aligned} B \cdot (x^2 \cdot y^2 - xy \cdot xy) &= (x + 2y)^2 \cdot (2x + 5y)^2 \\ &\quad - (x + 2y)(2x + 5y) \cdot (x + 2y)(2x + 5y) \\ &= (x^2 \cdot 4x^2 - 2x^2 \cdot 2x^2) \\ &\quad + (x^2 \cdot 2y^2 + 4y^2 \cdot 4x^2 - 2 \cdot 2x^2 \cdot 10y^2) + \dots \\ &= x^2 \cdot y^2 - xy \cdot xy \end{aligned}$$

2.5 Casimir Operator

The Killing form on a Lie algebra $\mathfrak{g}$ is defined in (Fulton and Harris 1991, pp. 206) as a symmetric bilinear form:

$$B(X, Y) = \mathrm{Tr}(\mathrm{ad}(X) \circ \mathrm{ad}(Y)).$$

The Casimir operator is defined in (Fulton and Harris 1991, p. 416) as follows. Let $U_1, \dots, U_r$ be a basis for $\mathfrak{g}$ and let $U_1', \dots, U_r'$ be its dual basis with respect to the Killing form. The Casimir operator is:

$$C = U_1 U_1' + \cdots + U_r U_r'.$$

It is also proved there that C acts as scalar multiplication on irreducible representation spaces of $\mathfrak{g}$.

2.6 Applications to Invariant Theory

The theory of representations of Lie algebras can be used to find invariants and covariants. Let $V = \mathbb{C}^n$ and let $\mathrm{SL}(V)$ act on the space of homogeneous polynomials of degree d, that is $S^d(V^*)$. For any $m \in \mathbb{N}$ we can extend the action of $\mathrm{SL}(V)$ to the larger space $S^m(S^d(V^*))$. Corresponding to this $\mathrm{SL}(V)$ representation is a $\mathfrak{sl}(V)$ representation. Using the previous theory we can decompose the vector space $S^m(S^d(V^*))$ into $\mathfrak{sl}(V)$ invariant subspaces. Using Theorem 3 this decomposition corresponds to a decomposition in $\mathrm{SL}(V)$ invariant subspaces. Now suppose that one of these subspaces happens to be isomorphic to $S^k(V^*)$ for some k. In that case, the projection

$$S^m(S^d(V^*)) \to S^k(V^*)$$

is an equivariant function.

The space $S^d(V^*)$ can be embedded equivariantly into $S^m(S^d(V^*))$.

Theorem 7 *Let V be $\mathbb{C}^n$. Suppose there exist integers m, d, k such that the space $S^m(S^d(V^*))$ contains an $\mathrm{SL}_n(\mathbb{C})$ invariant subspace W that is isomorphic to $S^k(V^*)$. Also suppose that there exists an element $f \in S^d(V^*)$ such that $f^{\otimes m} \in W$. Then there exists a polynomial covariant*

$$C\colon S^d(V^*) \to S^k(V^*)$$

of degree m.

Let $V = \mathbb{C}^3$. The following table gives all the small covariants and invariants whose existence has been demonstrated with this method. Entries marked with a star are contravariants. Zero corresponds with invariants. Note that some covariants map polynomials to polynomials of a higher degree. There are two straightforward ways to produce new covariants from old ones; if the spaces agree, covariants can be multiplied, or applied successively after each other. Covariants that can be obtained in this way are not listed. When there is more than one covariant of a particular degree we denote that as multiplicity $\cdot$ degree.

$d=2$	$m=2$	2^*
	$m=3$	0
$d=3$	$m=3$	3, 3^*
	$m=4$	0, 6^*,
	$m=5$	3^*
	$m=6$	0
$d=4$	$m=2$	4^*
	$m=3$	0, 6^*, 6
	$m=4$	2^*
	$m=5$	4^*, $2\cdot 2$, $2\cdot 8$
$d=5$	$m=3$	3, 3^*, 9
	$m=4$	4^*, 10^*, 2
	$m=5$	1, $3\cdot 5^*$, 11^*, $4\cdot 7$, $2\cdot 13$

2.6.1 Other Invariants that Can Be Obtained from Lie Algebras

An example of an invariant that is not a polynomial is the isomorphism type of the stabilizer Lie algebra of a form f, that is $\mathfrak{g}_f$.

$$\mathfrak{g}_f = \{X \in \mathfrak{sl}_3(\mathbb{C}) \mid X \cdot f = 0\}.$$

where $\cdot$ is the Lie algebra action induced on $S^n(V^*)$, see Subsection 2.2.2. (Clearly, for $g \in \mathrm{SL}(V)$, we have $\mathfrak{g}_{gf} = g\mathfrak{g}_f g^{-1} \cong \mathfrak{g}_f$.) This invariant is easy to compute, for the equations $X \cdot f$ and $\mathrm{trace}(X) = 0$ are linear in the indeterminates X_{ij}, forming the matrix X.

In particular the dimension of $\mathfrak{g}_f$ is an invariant. Unfortunately, for most (non-degenerate) f, this number is 0, and so $\mathfrak{g}_f$ is trivial. In that case, one knows that

the group stabilizer $\mathrm{SL}(V)_f$ is finite, but there is no efficient way known (to us) for computing its isomorphism type. (Of course the Gröbner basis algorithm solves the problem, but this solution often will be too demanding in computing resources.) A conceivable attack to determining the isomorphism type of the finite group would be to list the finite subgroups of $\mathrm{SL}_3(\mathbb{C})$ (they are known, see (Blichfeldt 1917; Feit 1982)) and to match their invariant forms of the right degree with the forms at hand. (Note that we propose here to use our equivalence algorithm to determine the group invariant which is the converse to what would have been useful for our purpose.)

2.7 The Null-Cone

Let $V = \mathbb{C}^n$ and let $f \in S^d(V^*)$. Suppose that the closure of the orbit of f (in the Zariski topology) under the action of $\mathrm{SL}(V)$ contains 0. Then all polynomial invariants will have the same value for 0 as for f. We see that such invariants cannot distinguish orbits that have 0 in their closures. The union of all those orbits is called the *null-cone*.

The weight vectors of the $\mathfrak{sl}_n(\mathbb{C})$ module $S^d(V^*)$ with respect to the usual maximal torus, are the monomials. The weight of ${x_1}^{d_1}{x_2}^{d_2}\cdots{x_n}^{d_n}$ can be given by a vector in $\mathfrak{h}^*$. It is $(d_1-d_2,\ldots,d_{n-1}-d_n)$. Given a polynomial f in $S^d(V^*)$ we define its *support*, denoted by $\mathrm{supp}\, f$, as the convex hull in $\mathfrak{h}^*$ of weights of the monomials of f. This is essentially the Newton polytope, only using different coordinates. By use of that terminology the null-cone can be characterized as follows:

Theorem 8 *Let $V = \mathbb{C}^n$ and consider $\mathrm{SL}(V)$ in its natural action on $S^d(V^*)$. Let $f \in S^d(V^*)$. There exists an $A \in \mathrm{SL}(V)$ such that $0 \notin \mathrm{supp}\, A \cdot f$ if and only if f lies in the null-cone.*

Proof: This result is a reformulation of the *Hilbert-Mumford Criterion*. See Proposition 5.3 in (Popov and Vinberg 1994, pp. 199). □

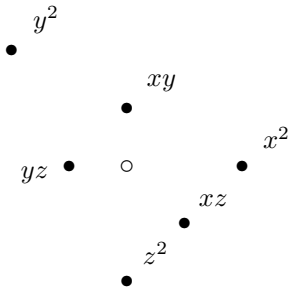
In the remainder of this section we will study what this means for the cases $n = 3$ and $d = 3, 4, 5, 6$. For the analysis of these forms we use the following definition from (Fulton 1969, pp. 66).

Definition 20 *Let f be any polynomial in two variables. Write $f = f_a + \cdots + f_b$, $a \le b$, where f_i is a form of degree i and $f_a \neq 0$. The* multiplicity *of f at $(0,0)$ is defined to be a. Write $f_a = \prod_i L_i^{r_i}$, where L_i is of degree 1. The lines L_i are called* tangent lines *to f at $(0,0)$.*

Remark: We let the same definition apply for points other than $(0,0)$ by translating the curve. Note that a singular point has multiplicity larger than 1.

We can characterize null-cones for various degrees, by first restricting the support using Theorem 8 and then giving a geometric interpretation of this restriction in the language of Definition 20.

Example: Let $d = 2$ and $n = 3$. Let f be a quadric in the null-cone. The monomials are $\{x^2, y^2, z^2, xy, xz, yz\}$. The picture below represents the monomial $x^{d_1}y^{d_2}z^{d_3}$ with the point $(d_1 - d_2, d_2 - d_3)$. The open circle is the origin. Note that the line through xy, z^2 contains the origin, as does the line through yz and x^2 and the line through y^2 and xz.



The maximal subsets of $\{x^2, y^2, z^2, xy, xz, yz\}$ of which the convex hull does not contain 0 are:

$$\begin{array}{ll} \{x^2, xy, y^2\}, & \{z^2, yz, xz\} \\ \{x^2, xz, z^2\}, & \{y^2, xy, yz\} \\ \{y^2, yz, z^2\}, & \{x^2, xy, xz\}. \end{array}$$

We may assume that the support of f is the convex hull of $\{x^2, xy, y^2\}$ or of $\{x^2, xy, xz\}$. Hence f can be written as the product of two lines. On the other hand, when the product of two lines is given, there exists an $\mathrm{SL}_3(\mathbb{C})$ transformation that maps these two lines to two lines of the above form. Hence a quadric lies in the null-cone if and only if it is the product of two lines.

2.7.1 Cubics

Let $d = 3$, $n = 3$. Let $f \in S^d(V^*)$ be an element of the null-cone. Using Theorem 8 and the fact that we can permute the variables, we may assume that f contains only the monomials x^3, x^2y, xy^2, y^2z and y^3. Going to the affine plane, we take $z = 1$. The point $(0, 0)$ is a singular point. We write $f = f_3 + f_2$ as follows:

$$\begin{aligned} f_3 &= a_{30}x^3 + a_{21}x^2y + a_{12}xy^2 + a_{03}y^3, \\ f_2 &= a_{02}y^2. \end{aligned}$$

If $a_{02} \neq 0$ then f has a point of multiplicity 2 with a double tangent (this case can correspond both to a cusp or a tacnode.) If $a_{02} = 0$ then f is the product of three lines. (The null-cone of cubics is characterized in (Popov and Vinberg 1994).)

2.7.2 Quartics

Let $d = 4$, $n = 3$. Let f be in the null-cone. The set of monomials does not have a unique largest convex part. Up to a permutation we need to consider two cases.
Case I. f is a linear combination of the following monomials: x^4, x^3y, x^2y^2, xy^3, x^3z, x^2yz, x^2z^2. Then f is reducible, it is the product of x and a polynomial of degree 3. We put $z = 1$ to go to the affine plane. Write $g = xf$. For g we write $g = g_3 + g_2 + g_1$ as follows:

$$\begin{aligned} g_3 &= a_{30}x^3 + a_{21}x^2y + a_{12}xy^2 + a_{03}y^3, \\ g_2 &= a_{20}x^2 + a_{11}xy, \\ g_1 &= a_{10}x. \end{aligned}$$

If $a_{10} \neq 0$ then $(0, 0)$ has multiplicity 1, with tangent x. Moreover, by substituting $x = 0$ we obtain that the line x meets f in an inflection point of f. If $a_{10} = 0$ then f has a point of multiplicity 2, such that x is a tangent that intersects in an inflection point. Summarizing case I: f is the product of a line and a cubic, where this line is tangent to the cubic in a point of inflection.

Case II. f is a linear combination of the monomials: x^4, x^3y, x^2y^2, xy^3, y^4, x^3z, x^2yz, xy^2z, y^3z. The affine case can be written as $f = f_4 + f_3$ as follows:

$$\begin{aligned} f_4 &= a_{40}x^4 + a_{31}x^3y + a_{22}x^2y^2 + a_{13}xy^3 + a_{04}y^4, \\ f_3 &= a_{30}x^3 + a_{21}x^2y + a_{12}xy^2 + a_{03}y^3. \end{aligned}$$

We see that f has a point of multiplicity 3 or higher.

2.7.3 Quintics

Let $d = 5, n = 3$. Assume that the quintic f lies in the null-cone. As for quartics there is not a unique largest convex part of $\mathfrak{h}^*$ in which we may assume f lies. We look at the two possible cases:

Case I. f is a linear combination of the monomials x^5, x^4y, x^3y^2, x^2y^3, xy^4, y^5, x^4z, x^3yz, x^2y^2z, xy^3z, y^4z. This corresponds to a point of multiplicity 4 or higher.

Case II. f is a linear combination of the monomials x^5, x^4y, x^3y^2, x^2y^3, xy^4, y^5, x^4z, x^3yz, x^2y^2z, x^3z^2.

The affine part of f is $f = f_5 + f_4 + f_3$, where:

$$\begin{aligned} f_5 &= a_{50}x^5 + a_{41}x^4y + a_{32}x^3y^2 + a_{23}x^2y^3 + a_{14}xy^4 + a_{05}y^5, \\ f_4 &= a_{40}x^4z + a_{31}x^3yz + a_{22}x^2y^2z, \\ f_3 &= a_{30}x^3. \end{aligned}$$

If $a_{30} \neq 0$ then f has a triple point, such that its three tangents are all equal; moreover, this tangent intersects f in only one point (but with multiplicity 5). If $a_{30} = 0$ then f has a point of multiplicity 4, such that two of its four tangent lines

are equal and moreover this double tangent intersects f in only one point (but with multiplicity 5).

The case $a_{30} = 0$ is contained in **Case I** so we may summarize the two cases as follows: f has a point of multiplicity 4 or higher or has a point of multiplicity 3, such that its three tangents are all equal and moreover this tangent intersects f in only one point (but with multiplicity 5).

2.7.4 Sextics

For $d = 6, n = 3$, there is one unique largest convex part in which we may assume a point f of the null-cone lies. Writing the affine part as $f = f_6 + f_5 + f_4$, we obtain that f_6 and f_5 are sextics and quintics of full generality but f_4 can be written as: $f_4 = a_{40}x^4 + a_{31}x^3y$. We conclude that f has a point of multiplicity 4 such that at least three of its four tangents are equal, or the curve has a point of multiplicity 5 or higher.

2.7.5 Singular Forms and the Null-Cone

In all of the above cases the forms in the null-cone are singular. We formulate this as a corollary to this discussion.

Corollary 1 *A non-singular polynomial in three variables, homogeneous of degree at most 6 does not lie in the null-cone.*

Chapter 3

The Symbolic Method

3.1 Introduction

Finding invariants becomes complicated very quickly as the degrees get higher. Not only is it hard to find them, even the simple act of writing them down becomes infeasible because the number of coefficients will be large. An invariant of degree m for homogeneous polynomials of degree d in n variables has

$$\binom{m + \binom{d+n-1}{d} - 1}{m}$$

coefficients. Even if half of them are zero this would still be an unwieldy high number.

What is needed is a notation in which an invariant can be written down in compressed form. If such a notation existed it might also facilitate the finding of such invariants. The shorter the notation the fewer possibilities need be considered. Such a notation was found by S. Aronhold at the end of the 19th century, see (O'Connor and Robertson ; Gurevich 1964). This method is known as (Aronhold's) *symbolic method*. Basically this method encodes a possible invariant in a string of numbers. The problem with this method is that, although it always gives invariants, in practice such invariants are often zero. And it is difficult to see in advance whether this will happen. Moreover, it is not always clear how basic algebraic or geometric constructions of invariants relate to the symbolic representation.

An invariant expressed with the symbolic method takes a negligible amount of storage compared to the same invariant written out in full. While this is a great advantage in the 21th century, in the 19th century when there were no computers, this advantage made the use of this method even more enticing. Looking at works like (Salmon 1877; Salmon 1879; Salmon 1862; Weyl 1946; Gurevich 1964; Gordan 1987), we get the impression that the symbolic method was systematically applied mostly to binary forms. The reason for this is no doubt the fast growing complexity. Modern computers make it possible to explore applications of the symbolic method

to more diverse parameters.

We use the notation and actions as defined in Subsection 1.2.3.

3.2 Brackets

In Section 3.3 we will introduce the umbral operator. It is a tool that can transform invariants for certain objects into invariants for other objects. Therefore in this section we will write down the relevant parts of invariant theory that we need in that section.

Let $V = \mathbb{C}^n$. Let X be an $m \times n$ matrix filled with the indeterminates x_{ij}, where we require $m \geq n$. Think of the rows of X as m points in the space V^*. We let $\mathrm{SL}(V)$ act on X in the natural way, an element $g \in \mathrm{SL}(V)$ acts on X as Xg^{-1}. This action extends to the polynomial ring $\mathbb{C}[x_{ij} \mid 1 \leq i \leq m, 1 \leq j \leq n]$. Our main goal in this section is to describe the elements of $\mathbb{C}[x_{ij}]^{\mathrm{SL}(V)}$.

Define the following set:

$$\Lambda(m,n) = \{[\lambda_1, \lambda_2, \ldots, \lambda_n] \mid 1 \leq \lambda_1 < \lambda_2 < \cdots < \lambda_n \leq m\}.$$

Elements of $\Lambda(m,n)$ are called *brackets*, the elements inside a bracket are called *symbols*. This set of brackets is the basis for a polynomial ring $\mathbb{C}[\Lambda(m,n)]$. Elements of the set $\mathbb{C}[\Lambda(m,n)]$ are called *bracket polynomials*. A *bracket monomial* or *tableau* is a product of brackets. We define an algebra homomorphism by

$$\begin{aligned} \delta_{m,n} \colon \mathbb{C}[\Lambda(m,n)] &\to \mathbb{C}[x_{ij}] \\ [\lambda_1, \ldots, \lambda_n] &\mapsto \det \begin{pmatrix} \text{row } \lambda_1 \text{ of } X \\ \text{row } \lambda_2 \text{ of } X \\ \cdots \\ \text{row } \lambda_n \text{ of } X \end{pmatrix}. \end{aligned}$$

We define the *bracket ring* $\mathcal{B}_{m,n}$ to be the image under $\delta_{m,n}$ of $\mathbb{C}[\Lambda(m,n)]$. The justification of these definitions lie in the fact that the bracket ring is a subring of $\mathbb{C}[x_{ij}]^{\mathrm{SL}(V)}$. The strict demands on brackets can be loosened somewhat. The homomorphism $\delta_{m,n}$ can be defined in the same way for brackets that are not sorted. For clarity, note that we have in that case: $\delta_{m,n}([1,2]) = -\delta_{m,n}([2,1])$. The image of a particular bracket polynomial L under $\delta_{m,n}$ is called its expansion.

Theorem 9 $\mathcal{B}_{m,n} \subset \mathbb{C}[x_{ij}]^{\mathrm{SL}(V)}$.

Proof: Let $L \in \mathbb{C}[\Lambda(m,n)]$ be a bracket. We need to prove that $\delta_{m,n}(L)$ is invariant under the action of $\mathrm{SL}(V)$. The theorem follows from this assertion. Let the symmetric group S_m act on $\mathbb{C}[\Lambda(m,n)]$ by permuting the symbols. Let S_m act on $\mathbb{C}[x_{ij}]$ by permuting the rows of X. The morphism $\delta_{m,n}$ respects these actions. We may therefore assume that $L = [1,2,\ldots,n]$, then we need to see that the determinant of an $n \times n$ matrix is invariant under the $\mathrm{SL}(V)$ action. But this is guaranteed by the multiplicative property of the determinant. □

Define $I_{m,n}$ to be the kernel of the map $\delta_{m,n}$; it is called the *ideal of syzygies*.

Theorem 10 (First Fundamental Theorem) *The bracket ring is isomorphic to the invariant subspace of* $\mathbb{C}[x_{ij}]$*, that is*

$$\mathbb{C}[\Lambda(m,n)]/I_{m,n} \cong \mathcal{B}_{m,n} = \mathbb{C}[x_{ij}]^{\mathrm{SL}(V)}.$$

Proof: A constructive proof is given in (Sturmfels 1993, pp. 85–89). The classic proof is in (Weyl 1946), a proof that works in all characteristics is in (de Concini and Procesi 1976). □

The ideal of syzygies $I_{m,n}$ is generated by the so-called Grassmann-Plücker relations (or syzygies). We describe them now. Let $A \in \Lambda(m, n+1)$, $A = [a_1, a_2, ..., a_{n+1}]$ and $B \in \Lambda(m, n-1)$, $B = [b_1, b_2, \ldots, b_{n-1}]$. The *Grassmann-Plücker relation* with respect to A and B, denoted by $[[AB]]$ is

$$\sum_{\tau=1}^{n+1} (-1)^{\tau} [a_1, \ldots, a_{\tau-1}, a_{\tau+1}, \ldots, a_{n+1}][a_\tau, b_1, b_2, \ldots, b_{n-1}].$$

The second bracket in this expression needs to be sorted, and the sign of the permutation should be added to that factor. In the case that a bracket contains an entry that occurs more than once, that bracket is taken to be zero.

Example: Take $m = 5, n = 3$, $L_1 = [2,3,4,5]$, $L_2 = [1,2]$. The Grassmann-Plücker relation $[[L_1 L_2]]$ becomes:

$$\begin{aligned}[3,4,5][2,1,2] - [2,4,5][3,1,2] + [2,3,5][4,1,2] - [2,3,4][5,1,2] = \\ - [2,4,5][1,2,3] + [2,3,5][1,2,4] - [2,3,4][1,2,5]\end{aligned}$$

The evaluation of the Grassmann-Plücker relation with parameters m and n with the map $\delta_{m,n}$ gives zero, that is, the relation is contained in $I_{m,n}$. It can therefore be used to rewrite bracket polynomials. This is expressed in the next theorem, a proof of which can be found in (Sturmfels 1993).

Theorem 11 (Second Fundamental Theorem) *The ideal of syzygies* $I_{m,n}$ *is generated by the set of Grassmann-Plücker relations:*

$$\{[[L_1 L_2]] \mid L_1 \in \Lambda(m, n-1), L_2 \in \Lambda(m, n+1)\}.$$

Using the ideal of syzygies one can find a basis for $\mathcal{B}_{m,n}$.

Definition 21 *Let* L *be a bracket monomial in* $\mathbb{C}[\Lambda(m,n)]$ *given by*

$$L = [\lambda_{11}, \lambda_{12}, \ldots, \lambda_{1n}][\lambda_{21}, \lambda_{22}, \ldots, \lambda_{2n}] \cdots [\lambda_{g1}, \lambda_{g2}, \ldots, \lambda_{gn}].$$

Then L *is a standard bracket monomial (or a standard tableau) if*

$$\begin{aligned} 1 \le \lambda_{i1} < \lambda_{i2} < \ldots < \lambda_{in} \le m \qquad & \text{for all } 1 \le i \le g \\ 1 \le \lambda_{1j} \le \lambda_{2j} \le \ldots \le \lambda_{gj} \le m \qquad & \text{for all } 1 \le j \le n. \end{aligned}$$

Theorem 12 *The image of the standard bracket monomials in* $\mathbb{C}[\Lambda(m,n)]$ *under* $\delta_{m,n}$ *is a vector space basis of the bracket ring* $\mathcal{B}_{m,n}$.

Proof: See (Sturmfels 1993, pp. 82). □

3.3 The Umbral Operator

Let $V = \mathbb{C}^n$. We want to find invariants for homogeneous polynomials of degree d. We think of these polynomials as points in the vector space $S^d(V^*)$. Polynomial functions on these polynomials, in particular invariant functions on these polynomials can be thought to live in the vector space $S^m\big(S^d(V^*)^*\big)$, see 1.3.1.

Before we define the umbral operator we need to introduce a basis for the various spaces we use. Let the standard coordinate functions $\{x_1, \ldots, x_n\}$ be a basis for V^*. Elements in $S^d(V^*)$ can be expressed as linear combinations of products in this basis. We use the following basis for $S^d(V^*)$:

$$\{\frac{d!}{\alpha_1!\alpha_2!\cdots\alpha_n!}x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n} \mid \sum_{i=1}^{n}\alpha_i = d\}.$$

The complicated scalar counts the number of different permutations of a monomial that are equal. It therefore reflects the way the symmetric tensor is built from general tensors. As a result most of the formulas we encounter later have much nicer coefficients. We denote the dual of this basis, a basis for $S^d(V^*)^*$, as follows:

$$\{a_{\alpha_1\alpha_2\cdots\alpha_n} \mid \sum_{i=1}^{n}\alpha_i = d\}.$$

Linear combinations of products of m of these basis elements gives the elements of $S^m\big(S^d(V^*)^*\big)$.

Let $\mathbb{C}[x_{ij}]_{(d,\ldots,d)}$ be the subspace $\mathbb{C}[x_{ij}]$ of those polynomials that are homogeneous of degree d in each row of X. We are now ready to introduce the *umbral operator*; it is the linear map determined by:

$$\phi\colon \mathbb{C}[x_{ij}]_{(d,\ldots,d)} \to S^m(S^dV^*)^* \tag{3.1}$$

$$\prod_{i=1}^{m}\prod_{j=1}^{n}x_{ij}^{v_{ij}} \mapsto \prod_{i=1}^{m}a_{v_{i1}v_{i2}\ldots v_{in}}. \tag{3.2}$$

Like $\delta_{m,n}$, this map respects the action of the symmetric group S_m on the rows of X. When we restrict ourselves to symmetrized polynomials this map is in fact a bijection, see (Sturmfels 1993). Let $\mathcal{B}_{m,n,d}$ be the subspace of $\mathcal{B}_{m,n}$ of those polynomials that are homogeneous of degree d in each of the rows of X.

Theorem 13 *The umbral operator induces a vector space isomorphism between* $\mathcal{B}_{m,n,d}^{S_m}$ *and the invariant subspace*

$$S^m\big(S^d(V^*)^*\big)^{\mathrm{SL}(V)}.$$

Proof: See (Sturmfels 1993, pp. 175). □

Next we need to describe the bracket polynomials that map to an element of $\mathcal{B}_{m,n,d}$.

Theorem 14 *Let $L = L_1 L_2 \cdots L_g$ be a bracket monomial such that $L_i \in \Lambda(m,n)$ for all i. If $\delta_{m,n}(L)$ is an element of $\mathcal{B}_{m,n,d}$ then $md = ng$ and each symbol $1, \ldots, m$ occurs precisely d times in the union of the brackets of L.*

Proof: Computing the determinant of a row that contains the symbol k, where $1 \leq k \leq m$ produces an element of $\mathbb{C}[x_{ij}]$ that is homogeneous of degree 1 in the variables of row k. On the other hand, the determinant of n rows other than row number k, do not contain any of the variables of row k. So in order for the complete multiplication to be homogeneous of degree d in row k, we need precisely d brackets that contain k.

So each of the elements $1, \ldots, m$ occurs d times. The argument can now be completed by double counting. The total number of elements in the g brackets of L is gn. On the other hand there are m symbols, each of which occurs d times, yielding md. □

Suppose we have a bracket polynomial l in $\mathbb{C}[\Lambda(m,n)]$ that maps to $\mathcal{B}_{m,n,d}$. One possibility is that all the bracket monomials, that l is a linear combination of, satisfy Theorem 14. If not then there is a bracket monomial in l that contains a symbol i that occurs more than d times. As a result all the terms in the umbral expansion of that bracket monomial contain an $a_{\alpha_1,\cdots,\alpha_n}$ for which the sum $\alpha_1 + \cdots + \alpha_n$ exceeds d. The only way such a bracket polynomial can map to $\mathcal{B}_{m,n,d}$ is if there are other bracket monomials that also contain a symbol that occurs more than d times. If we leave out those bracket monomials from l we obtain a bracket polynomial with the same evaluation. Therefore it suffices to find bracket monomials that satisfy the conditions of Theorem 14.

In this chapter we use the following parameters for bracket monomials: the integer n denotes the length of the brackets, m denotes the number of different symbols in the union of the brackets, d denotes the multiplicity of each symbol and g denotes the number of brackets.

If, after applying the umbral operator we have a non-zero result, then these parameters have an interpretation as well. The result is an invariant of degree m for polynomials in n variables that are homogeneous of degree d. Let an invariant corresponding to these parameters be C. The number g has the following property: for any $h \in \mathrm{GL}(V)$ and any polynomial f in n variables and of degree d we have that $C(h \cdot f) = \det(h)^g C(f)$. The number g is called the *index* of the invariant C.

We assume from now on that in all the bracket monomials each of the symbols occurs the same number of times. Moreover the variables n, d, m and g are always used with the meaning just given.

Example: We will look at an example computation. We are going to find an invariant of degree 2 for $\mathrm{SL}_2(\mathbb{C})$ acting on homogeneous polynomials in two variables

and of degree 2. We know already that such an invariant is the discriminant. The parameters in this case are: $n = 2$ (2 variables), $d = 2$ (polynomials of degree 2), $m = 2$ (invariant of degree 2), $g = 2$ (invariant has index 2). The only bracket with these parameters is $[1, 2]^2$. To evaluate this bracket monomial, we first compute $\delta_{2,2}([1, 2]^2)$. We need to take the square of the determinant of $X = (x_{ij})_{1\leq i,j\leq 2}$

$$\begin{aligned}\det\left(\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22}\end{pmatrix}\right)^2 &= (x_{11}x_{22} - x_{12}x_{21})^2 \\ &= x_{11}^2x_{22}^2 - 2x_{11}x_{22}x_{12}x_{21} + x_{12}^2x_{21}^2.\end{aligned}$$

In the next step we apply the umbral operator:

$$\begin{aligned} x_{11}^2x_{22}^2 &\mapsto a_{20}a_{02} \\ -2x_{11}x_{22}x_{12}x_{21} &\mapsto -2a_{11}^2 \\ x_{12}^2x_{21}^2 &\mapsto a_{02}a_{20}.\end{aligned}$$

Adding this together we obtain $2(a_{20}a_{02} - a_{11}^2)$. This is indeed an $\mathrm{SL}_2(\mathbb{C})$ invariant for the polynomials

$$a_{20}x^2 + 2a_{11}xy + a_{02}y^2.$$

3.3.1 Symmetrization of the Bracket Ring.

To find all invariants for polynomials we might do the following. First take an element from the bracket ring $\mathcal{B}_{m,n}$. Then compute its symmetrization under the action of the symmetric group S_m. Finally, if the preceding step did not produce zero, compute the image under the umbral operator. You are then guaranteed to get a non-zero invariant. Moreover, by Theorem 13 you get all the invariants in this way. If one follows this procedure for a basis of $\mathcal{B}_{m,n,d}$ then a spanning set for the invariants of degree d is obtained. Explicit bounds on the highest degree needed in a generating set for the invariant subspace are known, see (Derksen 1999).

Alternatively, we could skip the symmetrization and directly proceed with the umbral mapping. This gives the same result, only the order in which the terms are produced changes. The only advantage of symmetrizing is that way we would know in advance whether the result of the umbral mapping is zero or not. This is an important advantage as the umbral mapping is a very time consuming step.

Unfortunately the symmetrization is not always practical for anything but small values of m. For example, to compute invariants of degree 9 of quartics, as we will do later, we would need to perform symmetrization in $\mathcal{B}_{9,3,4}$, whose dimension exceeds 29000. The symmetric group itself in this case consists of 362880 elements.

For now we have decided that the advantages of full symmetrization do not balance the amount of extra computation time they involve. However, it would be interesting to try and adapt the symmetrization process to look only at a few large

subgroups of S_m. Let H be a subgroup of S_m and let L be a bracket monomial. Compute

$$\frac{1}{|H|}\sum_{h\in H} h\cdot L.$$

If this is zero, then the result of full symmetrization, or in fact the umbral operator will also be zero. In contrast with full symmetrization, the reverse result will not always hold. When full symmetrization would give zero, partial symmetrization might not.

It will take more time to symmetrize with respect to a larger group H. On the other hand, a larger group will also produce zero in more cases. Balancing the size of H with the amount of work the umbral operator costs will speed up (on the average) the process of deciding when a bracket monomial gives zero. Even a small group H can filter out a number of zero invariants in a relatively fast way. In fact one could view Lemma 5 as a simple first step in this direction.

Lemma 5 *Let L be a bracket monomial with d odd and $m \geq 2$. Let a and b be two distinct symbols, in the set $\{1,\ldots,m\}$. If each bracket of L that contains a also contains b, then the umbral evaluation of L is zero.*

Proof: Suppose we apply a permutation σ to the rows of X. The sum in the definition of the umbral mapping contains monomials of the following form:

$$\prod_{i=1}^{m} a_{v_{i1}v_{i2}\ldots v_{in}}.$$

After the permutation, this changes into

$$\prod_{i=1}^{m} a_{v_{\sigma(i)1}v_{\sigma(i)2}\ldots v_{\sigma(i)n}}.$$

However, since multiplication is commutative, this results in the same answer. What we have proved is that the umbral mapping is invariant under permutation. However a permutation on the rows of X can also be interpreted as a permutation of the symbols of L—it will have the same effect. Finally we examine the result of the permutation (a,b). On the one hand this cannot change the umbral evaluation. But on the other hand, the determinant that each row codes for is changed by a minus sign because, by hypothesis a and b are always in the same row. Hence the end result is multiplied with $(-1)^d$ which is not equal to 1 for odd d. In that case $\phi(L) = \phi(\sigma L) = -\phi(L)$, hence $\phi(L) = 0$. □

Remark: The previous lemma is not reversible; if d is odd then a bracket may well be zero but not satisfy the constraints of Lemma 5. Take for example the parameters $n = 3$, $d = 3$, $m = 5$, $g = 5$ and the bracket monomial:

$$L = [1,2,3][1,2,4][1,3,5][2,4,5][3,4,5].$$

This bracket monomial encodes an invariant of degree 5 for cubic forms. We know that such invariants do not exist (see (Popov and Vinberg 1994, pp. 146)), so it must be zero. That is $\phi(\delta_{m,n}(L)) = 0$. I know of no other way of proving that fact short of computing it or doing a full symmetrization. (Computation confirms that it is indeed zero.)

3.4 Evaluation of Bracket Monomials

Let n, m, d, g denote the number of variables, the degree of the invariant, the degree of the polynomials and the index of the invariant, respectively. Let L be a tableau conforming to these parameters. We know that such a tableau when evaluated as in Section 3.3, gives an invariant. Unfortunately this evaluation is computationally very intensive. First we describe how we arranged this to minimize computation time. Second we show some ideas that might be used to further speed up this computation.

3.4.1 Efficiency Aspects of Bracket Computations

Writing in a Maple like pseudo code, the general algorithm for evaluating a bracket monomial L, we will call it 'Algorithm 1', works like this.

(1) $S := 1$; $X := \text{matrix}(m, n)$;

(2) for i to g do $S := S * \det(X_{L[i]})$ od;

(3) umbral(S);

The term $X_{L[i]}$ means the matrix L with only the rows indicated by $L[i]$. The umbral operator in step 3 works by evaluating the terms of S in turn, as given by formula (3.1). The bottleneck in this algorithm is the huge number of terms S could get. To perform the umbral mapping we need to step through this list. Assuming all calculations are of order $O(1)$ then this algorithm takes $O(n!^g)$ time and space. On the bright side, during the expansions in step 2, a lot of terms are equal. These equal terms are added together and will reduce computation time in subsequent steps. On the other side however, the assumption that the elementary calculations can be done in time $O(1)$ is not true. As the objects grow larger a lot of time is spent on garbage collection. While doing computations with Maple we could reasonably compute invariants for which $(n!)^g \leq 2000$. This does not even include all invariants for cubics.

We can get an improvement of this algorithm by performing an umbral evaluation more frequently. As soon as there is a term $\prod_{ij} x_{ij}^{v_{ij}}$ in S and an i such that $\sum_j v_{ij} = d$, we can replace $\prod_{j=1}^{n} x_{ij}^{v_{ij}}$ with $a_{v_{i1}v_{i2}\ldots v_{in}}$. There are $\binom{d+n-1}{d}$ choices for a coefficient $a_{v_{i1}v_{i2}\ldots v_{in}}$ but there are m times as many choices for the corresponding coefficient $\prod_{j=1}^{n} x_{ij}^{v_{ij}}$. The fewer coefficients we have the greater the chance that two of them are equal and give a reduction in the number of terms. There is a

disadvantage to this method: every time a partial umbral evaluation is done all the terms of S have to be considered. This takes more time as the number of terms in S gets larger. This tradeoff leaves some room for improvement. Empirically we settled on the following algorithm, which we will call 'Algorithm 2'.

(1) $S := 1$; $X := \text{matrix}(m, n)$;

(2) for i to $d-1$ do $S := S * \det(X_{L[i]})$ od;

(3) for i from d to g do $S := S * \det(X_{L[i]})$; PartialUmbral(S); od;

When $(n!)^g$ is about 45000 this version is about ten times faster than the previous version. But even this improvement is not enough to handle the larger invariants we encountered. To say something about those we restricted ourselves to computing the invariants only for particular test polynomials. If one such a computation is not zero, we know that the corresponding invariant is not zero. By collecting results for a number of different test polynomials we can also answer questions about their independence. The change from the previous algorithm is again small. Every time we substituted a coefficient $a_{v_{i1}v_{i2}\ldots v_{in}}$ we replaced it with the value of the corresponding coefficient in the test polynomial. This is 'Algorithm 3'.

(1) $S := 1$; $X := \text{matrix}(m, n)$;

(2) for i to $d-1$ do $S := S * \det(X_{L[i]})$ od;

(3) for i from d to g do $S := S * \det(X_{L[i]})$;

(4) PartialUmbralAndSubstitute(S,f); od;

By choosing an f with a lot of zero terms this speeds up the process with a factor of about 25. Unfortunately the result carries less information. Instead of knowing the exact result we only get the value at one point. More information can be obtained by repeating the process with different test polynomials. To prove that a particular bracket monomial is non-zero, we need only find one test polynomial where its evaluation is non-zero. It is conceivable to have consistent bad luck in picking test polynomials. But fortunately, any invariant will, likely, be non-zero for a random polynomial.

It is also possible to use a hybrid between these last two versions, by using test polynomials of which some of the coefficients are indeterminates. The two extreme cases of this correspond to the original two algorithms—test polynomials without any indeterminate coefficients correspond to Algorithm 3 and a test polynomial with only indeterminate coefficients corresponds to Algorithm 2. This hybrid allows to selectively compute some coefficients of an invariant but not all. In spirit it is very similar to Algorithm 3, only slower; it proves that some invariant is not zero but it will usually not give the evaluation of all the coefficients in terms of those indeterminates. Still, knowing some coefficients may guide the search further by

giving insight where non-zero invariants are to be expected. An application of this idea is given in Section 3.7.

The table below is meant to illustrate the difference in computation time. It reports the time in seconds it took to compute the evaluation of these three brackets:

$$L_1 = [1,2,3][1,2,4][1,3,4][2,3,4],$$
$$L_2 = [1,2,3][1,2,4][1,3,5][2,4,6][3,5,6][4,5,6],$$
$$L_3 = [1,2,3][1,2,4][1,2,5][1,3,5][2,4,6][3,4,6][3,5,6][4,5,6].$$

For the last algorithm we used the test polynomial $x^3+y^3+z^3+3x^2y$ for L_1 and L_2 and $x^4+y^4+z^4+12x^2yz$ for L_3. The computation was done using Maple 5.1 on a Sun Sparc with Solaris 2.7 on a Ultra-Sparc 10, 333 Mhz processor with 128 Mb of memory. We repeated the computations three times and report here the average rounded to the nearest second.

Bracket	$(n!)^g$	Algorithm 1	Algorithm 2	Algorithm 3
L_1	1296	6	5	2
L_2	46656	2493	286	11
L_3	1679616		> 80000	51

The computation of bracket L_3 using Algorithm 2 was broken off after about a day of computation time. Algorithm 1 was terminated much sooner as it was not expected to produce a result in a reasonable time. For L_2 we will take a better look at the difference between these algorithms. Almost all the computation time is spent on the (partial) umbral evaluations. The time this takes depends linearly on the number of terms in the intermediate result, the variable S. In the next table we list the number of terms of S before and after the partial umbral evaluation. The first column lists the number of brackets that have been processed. The second column lists the number of terms in S after it was multiplied with the next (expanded) bracket but before the partial umbral evaluation. The third column lists the number of terms of S after partial umbral evaluation. The last two columns list these numbers for the third algorithm. Not all numbers are filled in for the first two rounds, to avoid cluttering the table. The numbers are the same for all these algorithms.

Round	Algorithm 1	Algorithm 2		Algorithm 3	
		Before	After	Before	After
1	6				
2	33				
3	174	174	174	174	44
4	927	927	564	237	52
5	4182	2478	954	235	36
6	16363	3676	103	133	1

It is interesting to compare the amount of work spent during umbral evaluation between Algorithm 1 and Algorithm 2. For the first this is proportional to 16363, since umbral evaluation is not done until the end. For Algorithm 2 this is proportional to the sum of the entries in column 2 (not counting the figures for round 1 and 2). The sum of column 2 is $174 + 927 + 2478 + 3676 = 7255$. So even though umbral evaluation is done four times as often, the amount of work is only 44%.

We have also tried another optimization, namely computing the invariant modulo a small prime. Note that such a prime cannot be to small because the expanded brackets tend to have coefficients that are divisible by a lot of small primes. Computing modulo 13 worked well for the sizes of brackets we attempted. It turned out however that this was hardly an improvement over the last algorithm. This is a bit surprising. When computing modulo a prime much more coefficients will be zero. This reduces the number of computations that need to be done in the next round. However most of the reduction of Algorithm 3 comes from the fact that a lot of terms can be added together. Computing modulo a prime does not increase this number. Still one could have expected a small gain here.

3.4.2 Non-sorted Tableau Evaluation

In this section we present the evaluation of brackets in a different way. That will allow us to make some statements about the resulting coefficients. In some special cases we can also determine the exact evaluation. Let L be a bracket monomial with parameters n, m, d and g.

Let $S_n^g = S_n \times \cdots \times S_n$ be the product of g copies of the symmetric group. Let $\sigma = (\sigma_1, \ldots, \sigma_g)$ be an element of S_n^g. Let S_n^g act on L by having σ_i acting on the i-th row, say $[x_1, \ldots, x_n]$ of L as follows:

$$\sigma_i \cdot [x_1, x_2, \ldots, x_n] = [x_{\sigma_i(1)}, \ldots, x_{\sigma_i(n)}].$$

Unless all of the σ_i are equal the identity, this transformation turns a standard tableau into a non-standard tableau. To σ we also attach a sign, namely $\operatorname{sign}(\sigma) = \prod \operatorname{sign}(\sigma_i)$. Let M be any, not necessarily standard, tableau. We define a map ψ that maps M to a monomial.

$$\psi\colon M \mapsto \prod_{i=1}^{m} a_{(\text{number of } i \text{ in column 1})\ldots(\text{number of } i \text{ in column n})}$$

Example: Let

$$L = [1,2,3][1,2,4][1,2,5][1,3,5][2,4,6][3,4,6][3,5,6][4,5,6].$$

First take $\sigma = (\mathrm{Id})^g$ and $M = \sigma \cdot L$. In this case we have $M = L$, since we transformed L with the identity. We calculate $\psi(M)$. First of all, there are four 1's in column 1 and no others, we obtain a_{400}. There is one 2 in column 1 and three 2's in column 2 hence a_{130}. Continuing in this fashion we find

$$a_{400}a_{130}a_{211}a_{121}a_{022}a_{004}.$$

For another example, we use the same bracket monomial but the following transformation:

$$\sigma = \big((),(),(),(2,3),(1,2,3),(1,3),(1,3),(1,2,3)\big).$$

Below we list M and $\sigma \cdot M$ next to each other. The rows of the bracket monomials are listed under each other to improve clarity.

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 4 \\ 1 & 2 & 5 \\ 1 & 3 & 5 \\ 2 & 4 & 6 \\ 3 & 4 & 6 \\ 3 & 5 & 6 \\ 4 & 5 & 6 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 4 \\ 1 & 2 & 5 \\ 1 & 5 & 3 \\ 6 & 2 & 4 \\ 6 & 4 & 3 \\ 6 & 5 & 3 \\ 6 & 4 & 5 \end{pmatrix}$$

Next we compute ψ.

$$\begin{aligned} \psi(\sigma \cdot M) &= a_{400}a_{040}a_{004}a_{022}a_{022}a_{400} \\ &= a_{400}^2 a_{040}a_{004}a_{022}^2 \end{aligned}$$

Theorem 15 *Let L be a tableau. The umbral evaluation of L equals*

$$\sum_{\sigma \in S_n^g} \operatorname{sign}(\sigma)\psi(\sigma \cdot L).$$

Proof: Let $L = [[a_{11}, \ldots, a_{1n}][a_{21}, \ldots, a_{2n}] \cdots [a_{g1}, \ldots, a_{gn}]]$. When this bracket monomial is evaluated into a polynomial in the variables x_{ij} we obtain:

$$\prod_{j=1}^{g}\Big(\sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \prod_{i=1}^{n} x_{a_{ji}\sigma(i)}\Big) = \sum_{\sigma \in S_n^g} \operatorname{sign}(\sigma) \prod_{j=1}^{g}\prod_{i=1}^{n} x_{a_{ji}\sigma_j(i)} \tag{3.3}$$

Applying umbral evaluation gives

$$\prod_{i,j} x_{ij}^{\nu_{ij}} \mapsto \prod_{i}^{m} a_{\nu_{i1}\nu_{i2}\cdots\nu_{in}}.$$

So to compute ν_{ab} we can fix $a_{ji} = a$ and count the number of times $\sigma_j(i) = b$, that is the number of b in column i of the permuted tableau. □

Example: Let $L = [1,2,3][1,2,4][1,3,4][2,3,4]$. This bracket monomial gives an invariant for cubics. This invariant is rather small and it can easily be computed in full on a computer—expanding the brackets into determinants only gives 415 terms. We will prove that this bracket monomial is not zero by evaluating one of

the coefficients. The coefficient we are going to compute is the coefficient of the monomial

$$a_{300}a_{030}a_{003}a_{111}.$$

If this coefficient is not zero, it should be possible to arrange the symbols in such a way that three elements from $\{1,2,3,4\}$ occur in only one column and the fourth symbol occurs in three different columns. We fix the first row and assume that one of the symbols is not fixed. Below we list the four basic solutions (brackets are listed as matrices for clarity).

$$\begin{pmatrix}1&2&3\\1&2&4\\1&4&3\\4&2&3\end{pmatrix}\quad\begin{pmatrix}1&2&3\\1&2&4\\1&3&4\\3&2&4\end{pmatrix}\quad\begin{pmatrix}1&2&3\\1&4&2\\1&4&3\\2&4&3\end{pmatrix}\quad\begin{pmatrix}1&2&3\\4&2&1\\4&1&3\\4&2&3\end{pmatrix}$$

The sign of the permutations that produce these four different tableaux are all -1. We now obtain all the solutions that give a contribution to the coefficient of the monomial we are computing. For each $\mu \in S_3$ we obtain a new solution by applying μ^4 to the solutions above. Since μ is applied four times the sign will still be -1. So there are $24 = 6 \times 4$ permutations of L that give the contribution -1. Hence the coefficient of $a_{300}a_{030}a_{003}a_{111}$ equals -24. A full evaluation of the bracket monomials confirms this computation.

Theorem 16 *The umbral evaluation of $M = [12\ldots n]^d$ is zero if and only if d is odd.*

Proof: First of all if d is even we can evaluate M for the test polynomials $x_1^d + \cdots + x_n^d$. Then, only monomials of the form

$$(a_{d0\cdots0}a_{0d0\cdots0}\cdots a_{0\cdots0d})$$

are not zero. Using the evaluation of Theorem 15 we find

$$\sum_{\sigma\in S_n}(\mathrm{sign}(\sigma))^d(a_{d0\cdot0}a_{0d0\cdot0}\cdots a_{0\cdots0d}) = n!.$$

Now suppose that d is odd. The symbols 1 and 2 always occur in the same row. Hence we can apply Lemma 5. We conclude that M is zero in that case. □

This construction gives an invariant for parameters that satisfy $m = n$ and $g = d$ with d is even. In other words there is an invariant for polynomials in n variables, homogeneous of even degree d that has a degree equal to n. In the case of binary forms, this invariant is the discriminant, i.e. the determinant of the matrix associated to the binary form, as in Section 1.3.

3.5 Invariants for Polynomials of Degree 3

In this section we will find the symbolic representation of invariants for homogeneous polynomials in 3 variables of degree 3. Let $V = \mathbb{C}^3$. From for example (Popov and Vinberg 1994) we know that the invariant ring of $S^3(V^*)$ is generated by an invariant of degree 4 and an invariant of degree 6.

First we look at the invariant of degree 4. The parameters are: $n = 3$, $d = 3$, $m = 4$ and $g = 4$. There are only four choices for these brackets, they are $[1, 2, 3]$, $[1, 2, 4]$, $[1, 3, 4]$ and $[2, 3, 4]$. Suppose we would use one of these brackets twice, say $[1, 2, 3]$, then 4 would occur three times in two brackets, hence it would occur twice in one bracket. In that case the whole expression would be zero. Therefore the only possibility left is:

$$[1, 2, 3][1, 2, 4][1, 3, 4][2, 3, 4].$$

A computation shows that it is indeed non-zero.

For the invariant of degree 6, there are a lot more possibilities. If we restrict ourselves to standard tableaux we get up to S_m isomorphism the following two non-zero bracket monomials.

$$[1, 2, 3][1, 2, 4][1, 3, 5][2, 4, 6][3, 5, 6][4, 5, 6]$$
$$[1, 2, 3][1, 2, 3][1, 4, 5][2, 4, 6][3, 5, 6][4, 5, 6]$$

Their umbral evaluations are equal. The invariants of degree 4 and degree 6 together generate the invariant ring of $S^3(V^*)$.

3.6 Invariants for Polynomials of Degree 4

Considering the invariants for homogeneous polynomials of degree 4 we first look at the Poincaré series (see (Shioda 1967)). The Poincaré series of the algebra of invariants encodes the dimension of the subspace of invariants that are homogeneous of a given degree. From it one can deduce how many invariants one needs to find, and of what degree, to have a generating set.

The numerator of the Poincaré series is:

$$\begin{aligned} 1 &+ z^9 + z^{12} + z^{15} + 2z^{18} + 3z^{21} + 2z^{24} + 3z^{27} + 4z^{30} \\ &+ 3z^{33} + 4z^{36} + 4z^{39} + 3z^{42} + 4z^{45} + 3z^{48} \\ &+ 2z^{51} + 3z^{54} + 2z^{57} + z^{60} + z^{63} + z^{66} + z^{75} \end{aligned}$$

and its denominator is:

$$(1 - z^3)(1 - z^6)(1 - z^9)(1 - z^{12})(1 - z^{15})(1 - z^{18})(1 - z^{27}).$$

The degrees in the denominator of this series correspond to a homogeneous system of parameters of the space of invariants, see (Dixmier 1987). The capacity of the computer we were working on limit us to bracket monomials with index about

12. In this case that corresponds to degree 9. Judging from this and the Poincaré series we should be able to find independent invariants of degree 3, 6, and two of degree 9. Of these the first three are listed in (Dixmier 1987), but in that paper they are given by a geometric construction. The following non-zero brackets were found, partly by guessing, partly by a systematic search.

$$[1,2,3]^4$$

$$[1,2,3][1,2,4][1,2,5][1,3,5][2,4,6][3,4,6][3,5,6][4,5,6]$$

$$[1,2,3][1,2,4][1,2,5][1,3,5][2,3,6][3,4,6][4,6,7][4,7,8][5,7,9][5,8,9]$$
$$[6,8,9][7,8,9]$$

$$[1,2,3][1,2,3][1,5,6][1,5,6][2,6,7][2,6,7][3,4,8][3,4,8][4,5,9][4,5,9]$$
$$[7,8,9][7,8,9]$$

It is possible for these invariants to be linearly dependent. To rule out that possibility we evaluated these invariants on four different test polynomials.

$$x^4+y^4+z^4+6x^2y^2+36xyz^2$$
$$x^4+y^4+z^4+12x^2yz$$
$$x^4+y^4+z^4$$
$$x^4+y^4+z^4+6x^2y^2+24xyz^2$$

We summarize the results in the following matrix. Each row gives the results for one test polynomial and all four invariants. Each listed in the same order as above.

$$\begin{pmatrix} 672 & 0 & -165888 & 10586112 \\ 6 & 48 & -18 & 318 \\ 6 & 0 & 0 & 6 \\ 312 & 0 & -12288 & 1156992 \end{pmatrix}$$

From this we see that the invariant of degree 6 is not equal to a multiple of the square of the invariant of degree 3. The two invariants of degree 9 are at least linearly independent. To rule out linear independence for all degree 9 invariants that can be obtained from these, replace the column for the degree 3 invariant with its cube and the column for degree 6 with the product of degree 6 and degree 3. We obtain thus:

$$\begin{pmatrix} 303464448 & 0 & -165888 & 10586112 \\ 216 & 288 & -18 & 318 \\ 216 & 0 & 0 & 6 \\ 30371328 & 0 & -12288 & 1156992 \end{pmatrix}$$

The determinant of this matrix equals 1585084524134400, proving independence.

3.7 Invariants for Polynomials of Degree 5

By decomposing the Lie algebra associated with the space $S^kS^5(V^*)$ we obtained that there exist two independent invariants of degree 6 for homogeneous polynomials

of degree 5. It is very likely that there exist a lot more invariants of higher degree but it is not feasible to decompose $S^k S^5(V*)$ for values of k higher than 8.

One finds a bracket monomial for the parameters $n = 3$, $d = 5$, $m = 6$, $g = 10$ rather quickly. For example the following bracket will do:

$$[1,2,3]^4[1,4,5][2,4,6][3,5,6][4,5,6]^3.$$

Finding a second bracket monomial that gives an invariant of degree 6 turned out rather hard. We used the following procedure.

First, using a backtracking algorithm, we generated a list of all possible standard tableaux with parameters $n = 3$, $d = 5$, $m = 6$, $g = 10$. Since d is odd, Lemma 5 applies so during this generation process we could discard all (possibly only half filled) tableaux if we knew in advance they would evaluate to zero. Even under these constraints there are still 96 candidate tableaux. They are too big to do a full evaluation. Using the test polynomial $x^5 + y^5 + z^5 + 5x^4y$ we found that the very first of these was not zero (its value was -6). It is the bracket shown above. To find the other invariant we went down the list of candidates and for each we computed their value for a few test polynomials. If these values were all zero we guessed the invariant was in fact identical to zero (to prove this one has to evaluate a lot more polynomials). And if on the other hand they were all equal to the corresponding values for the first bracket we concluded that we had found a different bracket to express the same invariant.

After about 20 bracket monomials were examined in this way (this took about half a week) we stopped this approach. Possibly the other invariant would have been found had we waited long enough. However, we will explain how we found the other invariant much faster. First we take a closer look at the bracket monomial we have already found. Evaluating the first bracket for the polynomial $ax^5+by^5+cz^5+5x^4y$ gives $-6b^2c^2a^2$. Since there exists an invariant independent of this one (we know this from the Lie decomposition above), there will also be an invariant where this term is zero. That is, where the coefficient of $a^2b^2c^2$ is zero. Although this invariant might not be expressible as a bracket monomial. Using the ideas in Subsection 3.4.2 we compute the coefficient of $a^2b^2c^2$ occurring in the evaluated bracket. We rewrite the above to show this. For clarity the rows of these brackets are listed below each other to form a matrix; on the left the original on the right the permuted version.

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \\ 1 & 2 & 3 \\ 1 & 2 & 3 \\ 1 & 4 & 5 \\ 2 & 4 & 6 \\ 3 & 5 & 6 \\ 4 & 5 & 6 \\ 4 & 5 & 6 \\ 4 & 5 & 6 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \\ 1 & 2 & 3 \\ 1 & 2 & 3 \\ 1 & 5 & 4 \\ 6 & 2 & 4 \\ 6 & 5 & 3 \\ 6 & 5 & 4 \\ 6 & 5 & 4 \\ 6 & 5 & 4 \end{pmatrix}$$

What we see here is a permutation of the rows such that each symbol only occurs in one column. In that case each symbol will represent the coefficient of x^5, y^5 or z^5. In this case the permuted bracket monomial represents $a^2b^2c^2$ (with the meaning of a, b and c as above). The presentation for that coefficient is essentially unique. We can permute the column to give us 6 in total. To prove that there are no other solutions we look at the following three rows that occur: $[1,2,3][1,4,5][2,4,6]$. We may assume that the first of these rows stays fixed. But in that case the other two rows are fixed as well. So the coefficient of $a^2b^2c^2$ is ± 6. We can determine the sign by looking at the signs of the permutations needed to transform the two matrices. Of the 12 signs, exactly 5 signs are -1. Hence the coefficient is -6.

Now this proves something we already know. But we can now try to restrict ourselves to bracket monomials that do not give -6. For example if a bracket contains the rows $[1,2,3][1,2,4][1,3,4]$ it is not possible to permute such that each symbol only occurs in one column. Hence the coefficient of $a^2b^2c^2$ is zero. We modified our backtracking algorithm to only find bracket monomials that start with the above three rows. There were six of those. Evaluating for a few test polynomials turned out that the third was non-zero. The bracket is:

$$[1,2,3][1,2,4][1,3,4][1,3,4][1,4,5][2,4,6][2,5,6][2,5,6][3,5,6][3,5,6].$$

Using the test polynomial $ax^5+by^5+cz^5+5(x^4y+y^4z+z^4x)$ the result is 60. The result for the same test polynomial using the previous bracket is $30-60abc-6a^2b^2c^2$. This confirms their independence.

3.8 Overview

We summarize all the invariants in symbolic form for polynomials of various degrees that we have found in Table 3.1 on Page 40.

3.9 Can a Standard Tableau Be a 2-Design?

The tableaux that give rise to invariants, by the symbolic method, have the properties of a 1-design. Here, we interpret the brackets as lines and the symbols as points. Two lines meet if they have a point in common. Since every symbol occurs d times, we have that any point lies on precisely d lines. This makes it a 1-design. (See (van Lint and Wilson 1992) for designs and their properties.) On the other hand a t-design can be interpreted as a tableau for any $t \geq 1$ but these will normally not be standard. Rewriting such a tableau as a sum of standard tableaux does not preserve the t-design property for $t > 1$.

We pose therefore the following question: Can a 2-design be a standard tableau? We will see that the answer is yes and find all the solutions. Unfortunately these do not give new invariants. By definition a 2-design has the property that any pair (a, b) of points with $a \neq b$ lies on the same number of lines as any other pair of unequal points.

n	d	m	g	Bracket monomial
2	2	2	2	$[1,2]^2$
2	3	4	6	$[1,2]^2[1,3][2,4][3,4]^2$
2	4	2	4	$[1,2]^4$
2	4	3	6	$[1,2]^2[1,3]^2[2,3]^2$
2	5	4	10	$[1,2]^2[1,3]^3[2,4]^3[3,4]^2$
3	2	3	2	$[1,2,3]^2$
3	3	4	4	$[1,2,3][1,2,4][1,3,4][2,3,4]$
3	3	6	6	$[1,2,3][1,2,4][1,3,5][2,4,6][3,5,6][4,5,6]$
3	4	3	4	$[1,2,3]^4$
3	4	6	8	$[1,2,3][1,2,4][1,2,5][1,3,5][2,4,6][3,4,6][3,5,6][4,5,6]$
3	4	9	12	$[1,2,3][1,2,4][1,2,5][1,3,5][2,3,6][3,4,6][4,6,7][4,7,8]$ $[5,7,9][5,8,9][6,8,9][7,8,9]$
3	4	9	12	$[1,2,3][1,2,3][1,5,6][1,5,6][2,6,7][2,6,7][3,4,8][3,4,8]$ $[4,5,9][4,5,9][7,8,9][7,8,9]$
3	5	6	10	$[1,2,3]^4[1,4,5][2,4,6][3,5,6][4,5,6]^3$
3	5	6	10	$[1,2,3][1,2,4][1,3,4]^2[1,4,5][2,4,6][2,5,6]^2[3,5,6]^2$

Table 3.1: Various invariants in symbolic form

First of all note that the following standard tableaux are 2-designs.

$$[1, 2, 3, \ldots, n]^g \tag{3.4}$$

$$([1, 2, \ldots, n-1][1, 2, \ldots, n-2, n] \cdots [2, 3, \ldots, n])^a \tag{3.5}$$

Theorem 17 *The only 2-designs that are also a standard tableau are the above two classes.*

Proof: We use the variables n, d, m, g to mean the number of variables, the degree of the polynomials, the degree of the invariant and the index of the invariant respectively. On the other hand they can also be interpreted to mean the number of points on a line, the number of lines through a point, the number of points and the number of lines. Let λ be the number of times a pair of points lies on a line. In traditional notation we are investigating $2-(m, n, \lambda)$ designs.

We now derive a number of relations among these parameters. When a tableau is standard the first d rows start with 1 and the last d rows end with n. Since this is also a design there will be an overlap of λ rows. Hence we have $g = 2d - \lambda$. The number of lines equals the number of lines through 1 plus the number of lines through n minus the number lines through 1 and n.

Furthermore we have the relations $md = ng$ and $\lambda(m-1) = d(n-1)$. These hold for all 2-designs. The first can be proved by counting the number of flags. The second can be proved by counting the number of triplets (a, b, l) where $a \in l$ and $b \in l \setminus \{a\}$. Using the first two relations to eliminate n from the last equation we get the following:

$$m(d-\lambda)^2 = (2d-\lambda)(d-\lambda).$$

So either we have $d = \lambda$ or we have

$$m = \frac{2d-\lambda}{d-\lambda}.$$

The case $\lambda = d$ corresponds to solutions of the kind $[1, \ldots, n]^g$. Therefore we assume $d \neq \lambda$.

Since m is an integer, $(d-\lambda)|(2d-\lambda)$. Therefore $d-\lambda|\lambda$. Put $d = \lambda + c$ where c is positive divisor of λ. Using the relations for the parameters we can express everything in terms of λ and c:

$$\begin{aligned} m &= 2 + \lambda/c & \qquad n &= 1 + \lambda/c \\ g &= 2c + \lambda & \qquad d &= \lambda + c. \end{aligned}$$

We see that the number of points is one more than the number of points on a line. Using the next lemma we obtain that this case corresponds to the second class of examples. □

Lemma 6 *A* $2-(k+1,k,\lambda)$ *design is of the form*

$$([1,2,\ldots,n-1][1,2,\ldots,n-2,n]\cdots[2,3,\ldots,n])^a.$$

Proof: All the lines contain all of the points except one. Let a_i be the number of lines that do not contain i. Counting the number of lines that contain 1 and 2 we obtain that $\lambda = g - a_1 - a_2$. Counting the number of lines that contain 1 and 3 we obtain $\lambda = g - a_1 - a_3$. Hence $a_2 = a_3$. In a similar vein we can prove that all the a_i are equal and the lemma follows. □

Chapter 4

Cubics

4.1 Introduction

In this section we will focus on cubic forms. Let $V = \mathbb{C}^3$, then cubic forms are seen as elements of $S^3(V^*)$, as in Subsection 1.2.4. On these forms there is an action of $H = \mathrm{SL}(V)$. We will touch briefly on the equivalence problem for this action. Then we will look at stabilizers for these forms and what they look like in general. We will use the Hessian normal form for cubics. There are different normal forms, among them the Weierstrass or the Lagrange normal form. We found that the Hessian normal form was more convenient. In any case the three forms can easily be transformed into one another. Also the theory of invariants of complex reflection groups is used. The chapter ends with some observations on the cohomology of this action.

4.2 The Hessian Normal Form

Denote the standard coordinate functions on V by x, y, z; these are also a basis for V^*. Let $f \in S^3(V^*)$, (see Subsection 1.2.4). The form f is in *Hessian normal form* if it can be written as $f = a(x^3 + y^3 + z^3) + bxyz$ for some a and b in $\mathbb{C}$. We define the *Hessian subspace* $L = \{a(x^3 + y^3 + z^3) + bxyz \mid a, b \in \mathbb{C}\}$, a two-dimensional linear subspace of $S^3(V^*)$.

Theorem 18 *For each non-singular cubic form f, there exists an element $g \in \mathrm{SL}_3(\mathbb{C})$ such that $g \cdot f \in L$.*

Proof: See (Brieskorn and Knörrer 1986, pp. 293). Note that g nor gf is unique, in general. □

Let f be a form in $S^3(V^*)$. To f we associate a curve in $\mathbb{P}^2(\mathbb{C})$, viz. $V(f) = \{[x, y, z] \mid f(x, y, z) = 0\}$. Projective points will be written with square brackets. The *points of inflection* of this curve are defined to be the points on $V(f)$ where the

determinant of the Hessian of f vanishes (see Equation (4.1) in Subsection 4.2.1). These are points on $V(f)$ where the tangent has an intersection with the curve of order 3. By Bézout's theorem cubics have nine inflection points. We denote the inflection points of the cubic f with $\mathbb{S}(f)$.

A remarkable property of the Hessian subspace, is that all its members contain the same nine inflection points. They are the solutions of the system $\{x^3+y^3+z^3 = 0, \quad xyz = 0\}$. Because of its importance we will call this set $\mathbb{S}$. The elements of $\mathbb{S}$ are:

$$\begin{array}{ccc} [0,1,-1], & [-1,0,1], & [1,-1,0], \\ [0,1,\eta], & [\eta,0,1] & [1,\eta,0], \\ [0,\eta,1], & [1,0,\eta] & [\eta,1,0]. \end{array}$$

Here $\eta^2 - \eta + 1 = 0$. Note that these nine points of inflection form a geometry, an affine plane of order 3.

Theorem 19 *A non-singular cubic f is in Hessian normal form if and only if $\mathbb{S}(f) = \mathbb{S}$.*

Proof: We did the 'only' if part. For the 'if' part, note that in fact f is in Hessian normal form if it contains all the points of $\mathbb{S}$. It will then turn out that these are the inflection points. □

4.2.1 Transforming a Cubic into Hessian Normal Form

Let f be a given cubic. How can we transform it into a Hessian normal form? There are at least two approaches to this problem. First of all, as we have seen, a form is in Hessian normal form if and only if its set of inflection points equals the set $\mathbb{S}$. This is the approach taken in (Brieskorn and Knörrer 1986, pp. 293). That reference contains an algorithm that can transform f to Hessian normal form when two of its inflection points are given. Also interesting in this regard is (Bix 1998); the algorithm given there can transform a real form to Weierstrass or Lagrange normal form if one real inflection point is given.

For this to work we need to find some of the inflection points. Inflection points are points where f intersects its Hessian. The latter is defined as:

$$\det \begin{pmatrix} f_{xx} & f_{xy} & f_{xz} \\ f_{xy} & f_{yy} & f_{yz} \\ f_{xz} & f_{yz} & f_{zz} \end{pmatrix}. \tag{4.1}$$

Solving a system of two forms of degree 3 will in general necessitate finding the roots of polynomial of degree 9. It is not possible to express the roots of a general polynomial of degree 9 in terms of its coefficients, using only roots and rational functions. This makes it necessary to work symbolically or numerically. An advantage of this method is that it not only gives the Hessian form, but also a transformation that can take f to a Hessian normal form.

Another approach to finding the Hessian normal form to which f is equivalent is through the use of invariants. There are two invariants for cubic forms in three variables. Written in the symbolic notation of Chapter 3, they are:

$$[1,2,3][1,2,4][1,3,4][2,3,4]$$
$$[1,2,3][1,2,4][1,3,5][2,4,6][3,5,6][4,5,6].$$

They are of degree 4 and 6, respectively. Since they are invariants, we should get the same values for f as for the Hessian normal form f is equivalent with. The values of these invariants for the form $a(x^3+y^3+z^3)+bxyz$ are:

$$\frac{1}{54}b^4 - 4a^3b \tag{4.2}$$
$$\frac{1}{972}b^6 - 6a^6 + \frac{5}{9}a^3b^3.$$

Let I_4 be the value of the invariant of degree 4 and I_6 the value of the invariant of degree 6. Using Gröbner basis computations we found the following relation:

$$0 = -108I_4^2 - 36I_4b^4 - 288b^2I_6 + b^8. \tag{4.3}$$

Replacing b^2 by c, we obtain a quartic in c. By first solving for c we can obtain all the solutions for b. From this we already see that the Hessian normal form is in general not unique. Relation (4.3) normally has eight solutions for b, each of which will lead to three solutions for a. That totals up to 24 Hessian normal forms for a general cubic. In Section 4.3 we will show this result from a different angle.

Example: As an example, let $f = x^2y + y^2z + z^2x$. We will bring it to a Hessian normal form. First we compute the two invariants mentioned above, this gives: $I_4 = 0$ and $I_6 = 162$. Substituting these values into (4.3), we obtain:

$$-46656b^2 + b^8,$$

which is equal to $b^2(b^6 - 6^6)$. Picking the solution $b = 6$ we obtain: $24 - 24a^3$, for which we could take $a = 1$. We conclude that the following two forms are equivalent:

$$x^2y + y^2z + z^2x$$
$$x^3 + y^3 + z^3 + 6xyz$$

Other choices for b and a would have given other forms. For example $b = 0$ and $a = \sqrt{-3}$ also gives a solution.

The next question regarding these two forms is giving the transformation that maps one of them to the other. In this specific case that is possible since the degree 9 polynomial is reducible. It would still involve some messy expressions however so we will not include them here.

With Equations (4.2) we can also compute the intersection of the null-cone with L. A Gröbner basis of the ideal generated by them with respect to the lexicographical ordering $b < a$ is:

$$\{11664a^6 - 7b^6, -b^4 + 216a^3b, b^7\}.$$

This implies that the only intersection point is $a = b = 0$.

4.3 Stabilizers of Cubics

Recall the Hessian subspace $L = \{a(x^3 + y^3 + z^3) + bxyz \mid a, b \in \mathbb{C}\}$. Let $N_H(L) = \{h \in H \mid hL = L\}$ and $Z_H(L) = \{h \in H \mid hl = l \; \forall l \in L\}$. Usually H will be $\mathrm{SL}(V)$ and in that case we will just write $N(L)$ or $Z(L)$. Let W be the quotient group $N(L)/Z(L)$. The group W acts on L in a natural way.

Lemma 7 *The group $Z(L)$ has order 27; it is isomorphic to $\mathbb{Z}_3^2 \rtimes \mathbb{Z}_3$.*

Proof: Let $g \in \mathrm{SL}_3(\mathbb{C})$. Then $g \in Z(L)$ if and only if $g \cdot (x^3+y^3+z^3) = x^3+y^3+z^3$ and $g \cdot (xyz) = xyz$. We will use these facts to determine all elements of $Z(L)$.

Assume that $g \in Z(L)$. Since $g \cdot (xyz) = xyz$ and since $\mathbb{C}[x, y, z]$ is a unique factorization domain, g must permute the subspaces $\langle x\rangle$, $\langle y\rangle$, $\langle z\rangle$. Therefore we can write $g = dp$, where d is a diagonal matrix and p is a permutation matrix.

From $g \cdot (x^3 + y^3 + z^3) = x^3 + y^3 + z^3$ we see that the entries on the diagonal of d are cubic roots of unity. From $g \cdot (xyz) = xyz$ we derive that the determinant of d should be 1. Finally because we are working in $\mathrm{SL}_3(\mathbb{C})$ the determinant of p should also be 1. Since there are nine ways to choose d and three to choose p, the order of $Z(L)$ is 27.

The subgroup of $Z(L)$ consisting of the diagonal matrices is normal, and its intersection with the group of permutation matrices is the identity. We conclude that that $Z(L) \cong \mathbb{Z}_3^2 \rtimes \mathbb{Z}_3$. □

Note that the group $Z_{\mathrm{GL}_3(\mathbb{C})}(L)$ is twice as large as the group $Z_{\mathrm{SL}_3(\mathbb{C})}(L)$, since there are six choices for p instead of three.

Now that we know the group $Z(L)$, we will try to find the group $N(L)$. For that purpose we first describe a subgroup $N' \subset N(L)$. Later we will show that in fact $N' = N(L)$. First we define the complex reflection subgroup $G = \langle S_1, S_2, S_3\rangle$ of $\mathrm{GL}_3(\mathbb{C})$, where

$$S_1 = S_{(e_1+e_2+e_3),\eta}, \qquad S_2 = S_{e_2,\eta}, \qquad S_3 = S_{e_3,\eta}.$$

Here η is a primitive cubic root of unity and $S_{v,\lambda}$ denotes a complex reflection such that $S_{v,\lambda}(v) = \lambda v$ and $S_{v,\lambda}(x) = x$ for all x orthogonal to v with respect to the standard hermitian inner product. The group G has order 648, see for example (Springer 1977).

All the curves that are defined by elements of L have the same set $\mathbb{S}$ of inflection points (see Theorem 19). The group G is easily seen to permute the set $\mathbb{S}$; also it

is straightforward to check that S_1, S_2 and S_3 map $x^3+y^3+z^3$ and xyz into L. So we obtain: $G \subset N_{\mathrm{GL}_3(\mathbb{C})}(L)$.

Although the group G is not a subgroup of $\mathrm{SL}_3(\mathbb{C})$, we can scale its elements so that it is. Let $N' = \{a \cdot M \mid M \in G,\, a^3 \det(M) = 1\}$. Since scalar multiplication with η is in G there are also 648 elements in N'. We have that $N' \subset N_{\mathrm{SL}_3(\mathbb{C})}(L)$.

Given this subgroup N' of N we can compute generators for $W' = N'/Z$. Then $W' \subset W$. Choose two basis vectors in L, viz. $f_1 = x^3+y^3+z^3$ and $f_2 = xyz$. Let ρ denote restriction to L. If $g \in G$ and $d^3 = \det(g)$ then for any $h \in L$ we have

$$\frac{1}{\det(g)}(\rho(g) \cdot h) = \rho(\frac{1}{d}g) \cdot h.$$

Expressing the transformations $\frac{1}{\det(S_i)}\rho(S_i)$ in the given basis we find the following matrices:

$$s_1 = \begin{pmatrix} \frac{1}{3}\eta + \frac{2}{3} & \frac{1}{9}\eta - \frac{1}{9} \\ 2\eta - 2 & \frac{2}{3}\eta + \frac{1}{3} \end{pmatrix}, \qquad s_2 = s_3 = \begin{pmatrix} \eta & 0 \\ 0 & 1 \end{pmatrix}.$$

A computation shows that s_1, like s_2 and s_3, is a complex reflection of order 3. We are now ready to prove that the groups N' and W' are in fact equal to N and W, respectively. The group W gives us precise control over de Hessian normal form. The orbit under W of an Hessian normal form are all the other normal forms that are equivalent with it.

Theorem 20 *The quotient group W is a complex reflection group of order* 24.

Proof: Above we have explicitly given a group N' such that $Z \subset N' \subset N$. Since $Z \lhd N$, we have $Z \lhd N'$ hence there is also a subgroup $W' = N'/Z$ of W that has $648/27 = 24$ elements. A computation showed that this group is a complex reflection group.

Let $f \in L$, $f \neq 0$. Let S and T be the two $\mathrm{SL}_3(\mathbb{C})$ invariants given in (Popov and Vinberg 1994, pp. 146). They have degree 4 and degree 6, respectively, and are not constant on L. All the elements of the orbit Wf of f in L give the same value when S or T is evaluated for them. Therefore using Bezout's theorem, the set

$$\{g \in L \mid g \text{ is equivalent to } f\}$$

can contain at most 24 elements. This is because these equivalent elements are solutions to $S(g) = S(f)$ and $T(g) = T(f)$, of which there are at most $6 \cdot 4$.

From the fact that $|Wf| \leq 24$ for all $f \in L$ we can prove that $|W| \leq 24$. Suppose, to derive a contradiction, that $|W| > 24$. First we prove that every element of L has a non-trivial stabilizing element in W. Let g be an arbitrary element of L. The orbit Wg contains 24 elements or less, so there are $w_1, w_2 \in W$ such that $w_1 g = w_2 g$. Hence $w_2^{-1} w_1$ is a non-trivial element of W that fixes g.

All the elements of the vector space L have a nontrivial stabilizing element. Let U be an infinite subset of L such that no two vectors are linearly dependent on each other. There is some element of the finite set W that fixes infinitely many elements of U. This element of W fixes a basis of L. In this case W would contain a point

that fixes L pointwise contradicting its construction. So $|W| \leq 24$. But $W' \subset W$ and $|W'| = 24$, hence $W = W'$. □

Remark: It follows from (Springer 1977), Cor. 4.2.12, that a complex reflection group of order 24 with invariants of degree 4 and 6 contains $4+6-2 = 8$ reflections. In this case they are:

$$s_1,\ s_1^2,\ s_2,\ s_2^2,\ s_1 s_2 s_1^{-1},\ s_1 s_2^2 s_1^{-1},\ s_2 s_1 s_2^{-1},\ s_2 s_1^2 s_2^{-1}. \tag{4.4}$$

Note that the two reflections s_1 and s_2 are related by $(s_1 s_2) s_1 (s_1 s_2)^{-1} = s_2$. A presentation of W with generators and relations is given by

$$\{x^3 = 1,\ y^3 = 1,\ xyx = yxy\}.$$

Checking that this group is indeed isomorphic to W was done in Gap (see (The GAP Group 1999)).

Remark: In Theorem 20 we noted that there are two invariants for the group W. Having an explicit representation for W it is easy to find these two invariants using Rademacher's construction (see (Cox, Little, and O'Shea 1997), Chapter 7). Let $a(x^3 + y^3 + z^3) + bxyz$ be an element of L. The following two expressions are invariant under the action of W on L:

$$b(6a - b)(6a - \eta b)(6a - \eta^2 b),$$

$$\prod_{i=0}^{2} (-3a + 3\sqrt{3}a - \eta^i b)(-3a - 3\sqrt{3}a - \eta^i b).$$

Expanding these expressions will, up to a multiple, give the Equations (4.2).

4.4 Affine and Projective Stabilizers

Based on the results of the previous sections we will determine the stabilizers of non-singular forms in $S^3(V^*)$ for the action of $\mathrm{SL}_3(\mathbb{C})$. Any non-singular form is equivalent to some form in Hessian normal form. Thus without loss of generality we can restrict ourselves to elements in the Hessian subspace L. Let $f \in L$ and $A \in \mathrm{SL}_3(\mathbb{C})$ such that $A \cdot f = \alpha f$ for some $\alpha \in \mathbb{C}$. A linear transformation maps an inflection point to an inflection point. In this case we apparently have $A \cdot \mathbb{S} = \mathbb{S}$. Hence $A \cdot L = L$. We have obtained that $A \in N(L)$.

We can thus further restrict ourselves to finding stabilizers of points in L for the action of N. The subgroup $Z(L)$ of $N(L)$ certainly stabilizes the points of L, hence we can finally restrict ourselves to finding stabilizers of points in L for the action of W.

This is easier because W is a finite group. If f is a non-singular cubic form and g is a Hessian normal form equivalent to f, then all the elements of the orbit Wg are equivalent Hessian normal forms.

The following theorem describes the stabilizers of reflection groups; it follows from (Steinberg 1964). For a reflection s_α let H_α denote the hyperplane that s_α leaves invariant.

Theorem 21 *Let l be a point of L. The subgroup of W generated by those reflections $s_\alpha \in W$ for which $l \in H_\alpha$ is the stabilizer in W of l.*

We apply this theorem to our case, using the list of reflections (4.4) in W given in Section 4.3. We find that up to scalar multiples there are four forms that lie on some H_α:

$$f_2, \quad f_1 - 3f_2, \quad f_1 - 3\eta f_2, \quad f_1 - 3\eta^2 f_2.$$

Since all four are reducible (each one of them can be factored into three linear factors), we obtain the following theorem:

Theorem 22 *The stabilizer in $\mathrm{SL}_3(\mathbb{C})$ of any non-singular f in $S^3(V^*)$ is isomorphic to $\mathbb{Z}_3^{\,2} \rtimes \mathbb{Z}_3$.*

An alternative proof to this theorem van be found in (Katz and Mazur 1985) where they use an approach based on the arithmetic of elliptic curves.

Next we determine the stabilizers of the cubic curves corresponding to a non-singular cubic form $f \in S^3(V^*)$. The stabilizer of a cubic f is contained in the stabilizer of its corresponding curve. But the latter might be larger. To differentiate between the two stabilizers we will call the latter the *projective stabilizer*.

The projective stabilizer of f is the group $\{h \in H \mid \exists \lambda \in \mathbb{C} : h \cdot f = \lambda f\}$. Again we can restrict ourselves to $f \in L$ and, since L is closed under scalar multiplication, we can also restrict ourselves to elements from W. If (a, b), representing the cubic $a(x^3+y^3+z^3)+bxyz$, is an eigenvector of an element $w \in W$ then so is each multiple of (a, b). Below we list each ratio b/a and the corresponding elements of W. The two ratios corresponding to the two eigenvectors of an element of W occur in the left column. In the right column each element of W occurs exactly once. There are two elements in W that fix a form of L in general, it is the column entry "–".

b/a	corresponding elements;
$0, \infty$	$s_2, s_2^2, s_1 s_2^2 s_1, s_1^2 s_2 s_1^2$
$-3 \pm 3\sqrt{3}$	$s_2 s_1 s_2, s_1^2 s_2^2 s_1^2$
$(-3 \pm 3\sqrt{3})\eta$	$s_1 s_2^2, s_2 s_1^2$
$(-3 \pm 3\sqrt{3})\eta^2$	$s_2^2 s_1, s_1^2 s_2$
$6, -3$	$s_2 s_1^2 s_2, s_1^2, s_1, s_2 s_1^2 s_2 s_1$
$6\eta, -3\eta$	$s_1^2 s_2^2, s_1 s_2^2 s_1^2, s_1 s_2 s_1^2, s_2 s_1$
$6\eta^2, -3\eta^2$	$s_2^2 s_1^2, s_1^2 s_2^2 s_1, s_1^2 s_2 s_1, s_1 s_2,$
–	$1, s_1 s_2^2 s_1 s_2^2$

The element $s_1 s_2^2 s_1 s_2^2$ is in the center of W and of order 2. This means that in general the stabilizer is isomorphic to $(\mathbb{Z}_3^{\,2} \rtimes \mathbb{Z}_3) \rtimes \mathbb{Z}_2 \cong \mathbb{Z}_3^{\,2} \rtimes S_3$, that is, the stabilizer from the previous section plus multiplication by -1.

Finally we will describe as abstract groups the various stabilizers occurring in the list above. First we look at the subgroup of $\mathrm{SL}_3(\mathbb{C})$ that stabilizes every curve obtained from a form in L. It is generated by the following elements:

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}, \quad \begin{pmatrix} \eta^i & 0 & 0 \\ 0 & \eta^j & 0 \\ 0 & 0 & \eta^{2(i+j)} \end{pmatrix}.$$

This group is isomorphic to $\mathbb{Z}_3^2 \rtimes S_3$. The special curves corresponding to the values in the table get an extra factor. For the curve $x^3 + y^3 + z^3 + \lambda xyz$ we have:

λ	Group
$(-3 \pm 3\sqrt{3})\eta^i$	$(\mathbb{Z}_3^2 \rtimes S_3) \rtimes \mathbb{Z}_2$
$6\eta^i, -3\eta^i$	$(\mathbb{Z}_3^2 \rtimes S_3) \rtimes \mathbb{Z}_3 \cong \mathbb{Z}_3^3 \rtimes S_3$
else	$\mathbb{Z}_3^2 \rtimes S_3$

4.5 Cohomology of Cubic Forms

Let k be a field of characteristic 0. Let K be a Galois extension of k, with Galois group $\mathrm{Gal}(K/k)$. We set $V = K^3$. We are looking at the action of $\mathrm{SL}_3(K)$ on cubic forms. Letting x, y, z denote a basis of V^*, we can express elements of $S^3(V^*)$ as polynomials in x, y, z.

Suppose we are given two forms f and h defined over k, and $g \in \mathrm{SL}_3(K)$ such that $gf = h$, so the forms f and h are equivalent over K, though not necessarily when considered over k. The group $\mathrm{Gal}(K/k)$ acts on $\mathrm{SL}(V)$ by acting on the entries in its matrix representation. Let $\sigma \in \mathrm{Gal}(K/k)$. Since f is defined over k the action of σ on f is trivial, that is $\sigma f = f$. We have:

$$\sigma(g)f = \sigma(gf) = \sigma(h) = h = gf,$$

hence $g^{-1}\sigma(g)$ is in the stabilizer of f. That is

$$g^{-1}\sigma(g) \in \mathrm{Stab}_{\mathrm{SL}_3(K)}(f) = \{g \in \mathrm{SL}_3(K) \mid gf = f\}.$$

We will write $\mathrm{Stab}(f) := \mathrm{Stab}_{\mathrm{SL}_3(K)}(f)$.

In general, for any $g \in \mathrm{SL}_3(K)$ with the property that $g \cdot f$ is defined over k we get a mapping from $\mathrm{Gal}(K/k)$ to $\mathrm{Stab}(f)$. This mapping is defined by $\sigma \mapsto g^{-1}\sigma g$. We will denote the image of σ by a_σ, so $a_\sigma = g^{-1}\sigma g$. Abusing notation, but following tradition we will also denote the map itself with a_σ. On the other hand, any $g \in \mathrm{SL}_3(K)$ such that $g^{-1}\sigma g \in \mathrm{Stab}(f)$ for all $\sigma \in \mathrm{Gal}(K/k)$ has the property that $g \cdot f$ is defined over k. The map a_σ has the following property.

Lemma 8 *The mapping a_σ defined as above satisfies $a_{\sigma\tau} = a_\sigma \sigma(a_\tau)$.*

Proof:

$$\begin{aligned} a_{\sigma\tau} &= g^{-1}\sigma(\tau(g)) \\ &= g^{-1}\sigma(gg^{-1}\tau(g)) \\ &= g^{-1}\sigma(g)\sigma(a_\tau) \\ &= a_\sigma\sigma(a_\tau) \end{aligned}$$

□

Definition 22 *A mapping* $a\colon \mathrm{Gal}(K/k) \to \mathrm{Stab}(f)$ *is a* cocycle *if it satisfies* $a_{\sigma\tau} = a_\sigma\sigma(a_\tau)$.

Define

$$Z^1(\mathrm{Gal}(K/k), \mathrm{Stab}(f)) = \{a \in \mathrm{Map}(\mathrm{Gal}(K/k), \mathrm{Stab}(f)) \mid a \text{ is a cocycle}\}.$$

We denote the identity of the group $\mathrm{Gal}(K/k)$ with 1. Observe that if a_σ is a cocycle, then $a_1 = 1$ since $a_1 = a_1^2$ and a_1 is invertible.

Let f be a cubic form defined over k. Suppose we have $g \in \mathrm{SL}_3(K)$ such that $g \cdot f$ is defined over k. This g gives rise to the cocycle a_σ. Suppose $m \in \mathrm{Stab}(f)$ and $h \in \mathrm{SL}_3(k)$. Then $(hgm) \cdot f$ will also be defined over k, it gives rise to the cocycle b_σ. We would like to consider these cocycles to be equivalent in some appropriate sense. They satisfy the following relation:

$$mb_\sigma = a_\sigma\sigma(m).$$

We prove this by checking that:

$$\begin{aligned} mb_\sigma &= m(hgm)^{-1}\sigma(hgm) \\ &= g^{-1}h^{-1}\sigma(h)\sigma(g)\sigma(m) \\ &= a_\sigma\sigma(m). \end{aligned}$$

In general, two cocycles a_σ and b_σ are said to be *cohomologous* (or cobounding) when there exists an $m \in \mathrm{Stab}(f)$ such that $mb_\sigma = a_\sigma\sigma(m)$. (See also (Husemöller 1987).) This relation is easily seen to be an equivalence relation. We define the cohomology set $H^1(\mathrm{Gal}(K/k), \mathrm{Stab}(f))$ to be the set Z^1 modulo the cobounding relation. A cohomology set is called trivial if it consists of only one element (the identity cocycle).

Theorem 23 *Let* $\rho \neq 1$ *be a cube root of unity. Let* $K = \mathbb{Q}(\rho)$ *and* $k = \mathbb{Q}$. *Define* $f = x^3 + y^3 + z^3 + \lambda xyz \in S^3k^* = k[V]_3$. *The set* $H^1(\mathrm{Gal}(K/k), \mathrm{Stab}(f))$ *is trivial.*

Proof: By Chapter 4 the elements in $\mathrm{Stab}(f)$ can be written as dp, where p is a power of the permutation matrix

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

and d is a diagonal matrix of the form

$$\begin{pmatrix} \rho^u & 0 & 0 \\ 0 & \rho^v & 0 \\ 0 & 0 & \rho^{2u+2v} \end{pmatrix},$$

where u and v are integers.

First we look at the elements of Z^1. The group $\mathrm{Gal}(K/k) = \langle\sigma\rangle$, where $\sigma(\rho) = \rho^2$. The order of σ is two. Let $a\colon \mathrm{Gal}(K/k) \to \mathrm{Stab}(f)$ satisfy $a_{\sigma^2} = a_\sigma\sigma(a_\sigma) = \mathrm{Id}$. Write $a_\sigma = dp$ where d is a diagonal matrix and p a permutation matrix as above. Then $a_\sigma\sigma(a_\sigma) = dp\sigma(dp) = dp\sigma(d)p = d(p\sigma(d)p^{-1})pp$. Since $d(p\sigma(d)p^{-1})$ is a diagonal matrix and p^2 is a permutation matrix, we must have $p^2 = 1$. However p has order 3 so $p = 1$. Hence if $a \in Z^1$ then we must have that a_σ is a diagonal matrix satisfying $a_\sigma^3 = \mathrm{Id}$.

The cocycle a_σ is cohomologous to the identity cocycle since $m = a_\sigma$ will satisfy the cobounding relation $ma_\sigma = \mathrm{Id}\sigma(m)$. □

Corollary 2 *Two non-singular Hessian cubic forms defined over* $\mathbb{Q}$ *are equivalent over* $\mathrm{SL}_3(\mathbb{Q})$ *if and only if they are equivalent over* $\mathrm{SL}_3(\mathbb{Q}(\rho))$.

Proof: This follows from the previous theorem and Proposition 1 in Chapter 3 of (Serre 1997). □

4.5.1 More Cohomology

For convenience we will work with $k = \mathbb{Q}(\rho)$. Let $f = x^3+y^3+z^3+\lambda xyz \in S^3k^*$, with $\lambda \in k$ and $\lambda \notin \{-3, -3\rho, -3\rho^2\}$ (so that f is not singular). Let K be a cyclic Galois extension of k, such that $[K : k] = 3$. The stabilizer of f under the action of $\mathrm{SL}_3(K)$ is given in Theorem 22. Two cocycles a_σ and b_σ are cohomologous if for some $m \in \mathrm{Stab}(f)$ we have $mb_\sigma = a_\sigma\sigma(m)$. But $\sigma(m) = m$ for all m in $\mathrm{Stab}(f)$. Therefore the cocycles a_σ and b_σ are cohomologous if and only if a_σ and b_σ are conjugates.

A Gap computation (see (The GAP Group 1999)) shows that the stabilizer of f has 11 conjugacy classes. Let a_σ be a representative in Z^1 of an element in H^1. First we solve the the equation $a_\sigma = g^{-1}\sigma(g)$ for $g \in \mathrm{SL}_3(K)$. If we succeed then $g^{-1}\sigma(g)f = f$, from which it follows that $\sigma(gf) = gf$ for all $\sigma \in \mathrm{Gal}(K/k)$, hence $gf \in \mathrm{SL}_3(k)$. On the other hand if gf and f are also equivalent over $\mathrm{SL}_3(k)$, then there exists an $h \in \mathrm{SL}_3(k)$ such that $gf = hf$. In that case $h^{-1}g \in \mathrm{Stab}(f)$, since $\mathrm{Stab}(f) \subset \mathrm{SL}_3(k)$ we obtain that $g = h(h^{-1}g) \in \mathrm{SL}_3(k)$. (see also Proposition 1 in Chapter 3 of (Serre 1997).)

As an example let $K = \mathbb{Q}(\sqrt[3]{2}, \rho)$, for brevity write $t = \sqrt[3]{2}$. We have that $|\mathrm{Gal}(K/k)| = 3$. In Table 4.1, each row corresponds to a conjugacy class. The first column lists a representative of some of the conjugacy classes of f. The second column lists a solution g to $a_\sigma = g^{-1}\sigma(g)$ when a_σ is equal to the element in the first column. The third column lists the results of applying this g to f. These forms are indeed defined over k instead of K.

Representative of conjugacy class	Solution to $a_\sigma = g^{-1}\sigma(g)$	$g \cdot (x^3+y^3+z^3+\lambda xyz)$
$\begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}$	$x^3+y^3+z^3+\lambda xyz$
$\begin{pmatrix} \rho & & \\ & \rho^2 & \\ & & 1 \end{pmatrix}$	$\begin{pmatrix} t & & \\ & t^2 & \\ & & \frac{1}{2} \end{pmatrix}$	$2x^3+4y^3+\frac{1}{8}z^3+\lambda xyz$
$\begin{pmatrix} \rho^2 & & \\ & \rho & \\ & & 1 \end{pmatrix}$	$\begin{pmatrix} t^2 & & \\ & t & \\ & & \frac{1}{2} \end{pmatrix}$	$4x^3+2y^3+\frac{1}{8}z^3+\lambda xyz$
$\begin{pmatrix} \rho & & \\ & \rho & \\ & & \rho \end{pmatrix}$	$\begin{pmatrix} t & & \\ & t & \\ & & \frac{t}{2} \end{pmatrix}$	$2x^3+2y^3+\frac{1}{4}z^3+\lambda xyz$
$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$	$\frac{\rho+2}{3}\begin{pmatrix} \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ t & \rho t & \rho^2 t \\ t^2 & \rho^2 t^2 & \rho t^2 \end{pmatrix}$	$-3/8(1+2\rho)\big((3+l)x^3+(48+16l)y^3+(96+32l)z^3+(144-24l)xyz\big)$

Table 4.1: Various forms equivalent over $\mathbb{Q}(\sqrt[3]{2},\rho)$ but not over $\mathbb{Q}$.

4.6 An Example of a Large Galois Group

Let $f = x^3+y^3+z^3+\lambda xyz$, with $\lambda \in \mathbb{Q}(\rho)\backslash\{-3,-3\rho,-3\rho^2\}$. The $\mathrm{Stab}_{\mathrm{SL}_3(\mathbb{C})}(f)$ is isomorphic to $\mathbb{Z}_3^2 \rtimes \mathbb{Z}_3$ (see Theorem 22, in Section 4.3) and defined over $\mathbb{Q}(\rho)$ (recall that $\rho^2+\rho+1=0$). Because of this we find it convenient to take $\mathbb{Q}(\rho)$ as our ground field. Given a Galois field extension $K/\mathbb{Q}(\rho)$ the associated cohomology group is determined by mappings from the Galois group to the stabilizer. Therefore it seems interesting to look at a field extension K such that $\mathrm{Gal}(K/\mathbb{Q}(\rho)) \cong \mathbb{Z}_3^2 \rtimes \mathbb{Z}_3$. We will now describe how we have found such an extension. We will also give two forms that are not equivalent over $\mathbb{Q}(\rho)$ but are over K.

First recall the fundamental Galois theorem (see (Lang 1965)). Let K be a Galois extension (normal and separable) of the field k. Let $G = \mathrm{Gal}(K/k)$ denote the fixed field of a subgroup $H < G$ with K^G.

Theorem 24 (Galois) *Let K be a finite Galois extension of k, with Galois group G. There is a bijection between the set of subfields of E of K containing k, and the set of subgroups H of G, given by $E = K^H$. The field E is Galois over k if and only if H is normal in G, and if that is the case, then the map $\sigma \mapsto \sigma|E$ induces an isomorphism of G/H onto the Galois group of E over k.*

4.6.1 Constructing the Field Extension K

Let G be the group $\mathbb{Z}_3^2 \rtimes \mathbb{Z}_3$. What we are looking for, is a field K such that $\mathrm{Gal}(K/\mathbb{Q}(\rho)) = G$. Let H equal one of the normal subgroups of G that are isomorphic to $\mathbb{Z}_3^2$. If we suppose that the field K with the required properties exists then taking $K_1 = K^H$ we get $\mathrm{Gal}(K_1/\mathbb{Q}(\rho)) \cong \mathbb{Z}_3$ and $\mathrm{Gal}(K/K_1) \cong \mathbb{Z}_3^2$. We will first construct K_1, a degree 3 extension of $\mathbb{Q}(\rho)$. Then we construct K as an extension of K_1. Adjoining any third root to $\mathbb{Q}(\rho)$ gives a Galois extension of degree 3. We put $K_1 = \mathbb{Q}(\rho, \sqrt[3]{2})$.

Let K_2 be an extension K_1, defined as the splitting field of $(x^3-1)^3-2$. It turns out that $\mathrm{Gal}(K_2/\mathbb{Q}(\rho)) \cong \mathbb{Z}_3^3 \rtimes \mathbb{Z}_3$. Dividing this group by its center (which is of order 3) gives the desired group. If s is an element of this center then $K = K_2^{\langle s \rangle}$. We can construct this fixed field. An automorphism s with these properties is given by:

$$\sqrt[3]{\rho^i \sqrt[3]{2}+2} \mapsto \rho \sqrt[3]{\rho^i \sqrt[3]{2}+2}, \quad \text{for } i = 0,1,2.$$

The field K is generated by elements of the form $x+s(x)+s^2(x)$. Put $a = \sqrt[3]{\sqrt[3]{2}+1}$, $b = \sqrt[3]{\rho\sqrt[3]{2}+1}$, $c = \sqrt[3]{\rho^2\sqrt[3]{2}+1}$. The field K can be generated as follows:

$$K = \mathbb{Q}(\rho, \sqrt[3]{2}, a^2b, a^2c, b^2a, b^2c, c^2a, c^2b).$$

This representation can be simplified, using the fact that $(abc)^3 = 3$ and $(a^2b)^3 + (a^2c)^3 = 3\sqrt[3]{2}$. We obtain: $K = \mathbb{Q}(\rho, \sqrt[3]{2}, \sqrt[3]{3}, a^2b)$.

4.6.2 Construction of two Forms

We want to construct two cubic forms f and h over $\mathbb{Q}(\rho)$ such that they are not equivalent over $\mathbb{Q}(\rho)$ but are equivalent over K. Let $g \in \mathrm{SL}_3(K)$ such that $g \cdot f = h$. For any element σ of $\mathrm{Gal}(K/\mathbb{Q}(\rho))$ we have that $\sigma(g \cdot f) = \sigma(h) = h = g \cdot f$ and $\sigma(g \cdot f) = \sigma(g) \cdot \sigma(f) = \sigma(g) \cdot f$. The g we are looking for must have the property that for all σ, $g^{-1}\sigma(g) \in \mathrm{Stab}(f)$. In this case the mapping $\sigma \mapsto g^{-1}\sigma(g)$ is a homomorphism since $g^{-1}\sigma(g)g^{-1}\tau(g) = g^{-1}\sigma(g)\sigma(g^{-1}\tau(g)) = g^{-1}\sigma(\tau(g))$. Hence it suffices to find such a g for generators of the Galois group. We obtained the following matrix:

$$g = \begin{pmatrix} \frac{a^2b}{\delta} & \frac{b^2c}{\delta} & \frac{c^2a}{\delta} \\ a^5c & b^5c & c^5a \\ a^8b & b^8c & c^8a \end{pmatrix}.$$

Here $\delta = -18-36\rho$ is chosen such that the determinant of the matrix is 1. Applying this matrix to the form $x^3 + y^3 + z^3 + \lambda xyz$ gives:

$$\begin{aligned} &486(-3 + 6\rho + \lambda + 2\lambda\rho)x^3 + 54\lambda x^2y + 162x^2y\rho - 27\lambda zx^2 + 81zx^2 + \\ &3xy^2 - \lambda xy^2 + 15pxy^2 - 2\rho\lambda xy^2 + \lambda xyz - 12\rho zxy + 2\rho\lambda xyz - \frac{1}{6}\lambda z^2x - \\ &\frac{1}{2}z^2x - \frac{1}{3}\rho\lambda z^2x + 2\rho z^2x - \frac{1}{54}(-13 - 8\rho + \lambda)y^3 + \frac{1}{27}\lambda zy^2 - \frac{2}{9}zy^2 - \\ &\frac{1}{6}zy^2\rho - \frac{1}{54}\lambda z^2y + \frac{1}{18}z^2y + \frac{1}{18}z^2y\rho + \frac{1}{324}(-1 - 2\rho + \lambda)z^3. \end{aligned}$$

Indeed all its coefficients are in $\mathbb{Q}(\rho)$.

Chapter 5

Quartics

5.1 Introduction

In this chapter we focus on the equivalence problem for quartics. To be more precise, we consider the following problem. Given two homogeneous polynomials of degree 4, in three variables, does there exist an element in $\mathrm{SL}_3(\mathbb{C})$ that transforms one of them into the other? And if there does exist such a transformation, can we find it? We might call the first aspect the decision problem and the second the construction problem. In general these are hard problems.

One approach to the decision problem consists of using invariants. If there exists an invariant that gives a different value for both forms then we know that they are not equivalent. On the other hand, if the values for these two polynomials agree for all possible invariants and if at least one of these invariants is not zero then they are equivalent. Unfortunately if all invariants are zero then the two polynomials may or may not be equivalent. The set of polynomials for which this is true is called the *null-cone*. Fortunately, non-singular polynomials do not lie in the null-cone. One could say that the decision problem is solved in principle for the class of non-singular forms. This is true since in principle it is possible to compute all invariants, using for example the symbolic method of Chapter 3. Note that it would be hard to move from this solution 'in principle' to an actual solution. For quartics invariants would be needed up to degree 75. The highest degree of an invariant for quartics in an independent set, explicitly known to us, is 27. Moreover, apart from finding these invariants, that is giving descriptions of them, it is a different matter to write them out in full. The mentioned invariant of degree 75 has 7632612327410136 terms (some of which could be zero).

Invariants can be very practical though. If we are given two *random* polynomials then it is likely that they are not equivalent. And this can be verified almost certainly with an invariant of low degree, some of which are given in Chapter 3.

For the construction problem invariants are not very helpful. Although it is sometimes possible to express the transformation matrix in terms of values of cer-

tain invariants, this relation is often an implicit polynomial relation of high degree. Moreover it is not apparent how this relation is to be constructed in general.

Another approach consists of using general equation solving mechanisms. For example, one could transform the first of the two polynomials with a general element of $\mathrm{SL}_3(\mathbb{C})$. The assertion that the transformed polynomial is equal to the other polynomial, translates to a set of polynomial equations in the terms of the transforming matrix. After that one could try to solve this set of equations, for example by computing a Gröbner basis with a lexicographic ordering on the indeterminates, see (Cox, Little, and O'Shea 1997). This approach is certainly viable for problems of low degree and with few variables. However, in general the Gröbner basis computation might need an exponential amount of memory compared to the input, see (Mayr and Meyer 1982). Therefore it becomes increasingly less feasible for more complex problems. In particular, experiments along these lines for quartics have shown that this approach will not (often) work. Still, an advantage of this method is its flexibility. For example, as soon as some restriction is known for the transformation we are looking for, it is easy to add these to the set of equations.

Still another approach is that of looking for normal forms. For example, as shown in Chapter 4, there is a normal form for cubics. That is, there is a class of cubics with the property that it intersects the orbit of an arbitrary cubic precisely once or at most a finitely many (but globally bounded) number of times. Elements of such a class are said to be in normal form. Now, to find out whether two given forms are equivalent it would suffice to transform them both to a normal form. Comparing these two normal forms would then decide whether they are equivalent or not. If this transformation to a normal form is done with an explicit transformation this will then also solve the construction problem. This approach has the added charm that it is likely to give additional theoretical benefit. For a lot of problems it would suffice to only study the normal forms, since a lot of properties of forms are preserved by linear transformations. Such a linear normal form is called a *Weierstrass section*. It follows from the theory (Popov and Vinberg 1994) that such a normal form does not exist for quartics. The absence of such a form makes this approach much less attractive.

It seems that yet another approach is needed, or at the very least, it should be interesting to see why this problem is so hard. In this chapter an algorithm is outlined that will often transform the construction problem for quartics in three variables to a construction problem for quartics in only two variables. Since the latter is a subproblem of the former this is a step forward. The downside is that the latter problem is essentially equivalent to computing the roots of a quartic in one variable. This can be done by adjoining the roots of the polynomial to $\mathbb{Q}$ or more explicitly adjoining a sequence of roots. This equivalence problem can therefore be solved. Of course, if one is only interested in a numerical solution, the problem indeed becomes substantially easier.

Smooth quartic curves belong to the class of genus 3 curves. Conversely, 'most' genus 3 curves (precisely: the non-hyperelliptic (smooth) genus 3 curves) embed in $\mathbb{P}^2$ as quartic curves through the canonical linear system. The space of quartic

curves can be used to construct the moduli space $\mathcal{M}_3$ of genus 3 curves. This moduli space has dimension 6, as the following parameter count indicates: The (projective) space of quartic curves has dimension $14 = \binom{4+2}{2} - 1$ whereas $\dim(\mathrm{SL}_3) = 8$. The role of invariants in this context is that they may be of help in understanding the space $\mathcal{M}_3$ (see (Faber 1990) for more on this moduli space).

In this chapter V is a vector space with basis e_1, e_2, e_3. The dual basis is given by x, y, z. Quartics will be identified with the points of $S^4(V^*)$ as described in Subsection 1.2.4. The action of $\mathrm{SL}(V)$ on quartics is described in Subsection 1.2.3.

5.2 Determining Equivalence

5.2.1 Overview of the Algorithm

We will describe an algorithm that can solve the equivalence problem for regular quartics. We will define the term regular in the proof; it is a series of invariants that should not be zero.

Theorem 25 *Given two regular quartics f_1 and f_2, there exists an algorithm that decides whether they are equivalent, and if so, finds an $H \in \mathrm{SL}_3(\mathbb{C})$ such that $Hf_1 = f_2$.*

The theorem follows from the following:

Theorem 26 *Let f_1 and f_2 be two regular polynomials in 3 variables, homogeneous of degree 4. The following algorithm produces two polynomials g_1 and g_2 homogeneous of degree 4 but in 2 variables and a map $\alpha\colon \mathrm{SL}_2(\mathbb{C}) \to \mathrm{SL}_3(\mathbb{C})$, such that f_1 and f_2 are equivalent if and only if there exists an $A \in \mathrm{SL}_2(\mathbb{C})$ such that $Ag_1 = g_2$ and $\alpha(A)f_1 = f_2$. Moreover there are at most finitely many A for which $Ag_1 = g_2$.*

In this section we will give an outline of the algorithm. In the remainder of this chapter we will go deeper into the steps thereby proving the claim of the theorem. At the end of chapter we also give an example. Let f_1 and f_2 be two elements of $S^4(V^*)$.

(1) (subsect. 5.2.2) There exists a covariant $\mathrm{cov}\colon S^4(V^*) \to S^2(V)$. Compute $Cf_1 := \mathrm{cov}(f_1)$ and $Cf_2 := \mathrm{cov}(f_2)$.

(2) If the discriminant of Cf_1 is not equal to the discriminant of Cf_2 then return that f_1 and f_2 are not equivalent. If the discriminant of Cf_1 and Cf_2 are both zero, report that the algorithm failed.

(3) (subsect. 5.2.3) We may assume that the discriminant of Cf_1 and Cf_2 is 1 (for if they are not we can scale the forms so that they are). Compute $A_1, A_2 \in \mathrm{SL}_3(\mathbb{C})$ such that $\mathrm{cov}(A_1 f_1) = \mathrm{cov}(A_2 f_2) = e_1^2 + e_2^2 + e_3^2$ (note that Cf_1 and Cf_2 are written down with respect to the basis of V instead of V^*).

(4) (subsect. 5.2.4) Restrict $\mathrm{SL}_3(\mathbb{C})$ to its subgroup that leaves the above mentioned quadric form invariant. That subgroup is $\mathrm{SO}_3(\mathbb{C})$. We parameterize this latter group by $\mathrm{SL}_2(\mathbb{C})$.

(5) (subsect. 5.2.5) Map $A_1 f_1$ and $A_2 f_2$ to $S^4(\mathbb{C}^2)$. In this space there exists a normal form. Compute B_1 and B_2 such that $B_1 A_1 f_1$ and $B_2 A_2 f_2$ map to the same normal form. If this is impossible, return that f_1 and f_2 are not equivalent (this is Lemma 3).

(6) If $B_1 A_1 f_1 = B_2 A_2 f_2$, report that f_1 and f_2 are equivalent, otherwise report that they are not. In the case of equivalency, report that the transformation $A_2^{-1} B_2^{-1} A_1 B_1$ maps f_1 to f_2.

5.2.2 Covariant

The first step is to use a classical covariant, $\mathrm{cov}\colon S^4(V^*) \to S^2(V)$, reference to this covariant can be found in (Salmon 1879). For the sake of completeness its construction is given here now, mostly following (Dixmier 1987).

Let $f \in S^4(V^*)$ be given as

$$\begin{aligned} &a_{400}x^4 + a_{310}4x^3y + a_{220}6x^2y^2 + a_{130}4xy^3 + a_{040}y^4 \\ &+a_{301}4x^3z + a_{211}12x^2yz + a_{121}12xy^2z + a_{031}4y^3z \\ &+a_{202}6x^2z^2 + a_{112}12xyz^2 + a_{022}6y^2z^2 \\ &+a_{103}4xz^3 + a_{013}4yz^3 \\ &+a_{004}z^4. \end{aligned}$$

Furthermore, let the binary form $g \in S^4(\mathbb{C}^2)$ be given by

$$a_{40}x^4 + a_{31}4x^3y + a_{22}6x^2y^2 + a_{13}4xy^3 + a_{04}y^4.$$

An invariant for the action of $\mathrm{SL}_2(\mathbb{C})$ on the latter form is given by the following determinant:

$$\begin{vmatrix} a_{40} & a_{31} & a_{22} \\ a_{31} & a_{22} & a_{13} \\ a_{22} & a_{13} & a_{04} \end{vmatrix}. \tag{5.1}$$

It is known as the *Hankel determinant*, see for example (Popov and Vinberg 1994). We can also express this invariant with the symbolic method, used in Chapter 3; it is

$$\frac{1}{6}[1,2]^2[1,3]^2[2,3]^2.$$

This invariant is zero if and only if the roots of g form a harmonic range. We can transform this invariant to a covariant $\psi\colon S^4(V^*) \to S^6(V)$ of degree 3, as follows: Let $f \in S^4(V^*)$ be given. For any $l \in V = V^{**}$, we can restrict f to points $\bar{x} = (x, y, z)$ such that $\bar{x}(l) = 0$. This gives an element in $S^4(\mathbb{C}^2)$. The set of l for which this binary quartic gives zero when invariant (5.1) is evaluated lies on

a degree 6 surface. In this way, to each element of $S^4(V^*)$ there is an associated element of $S^6(V)$. This gives a covariant of degree 3.

Next, this covariant can be transformed to the covariant we need in this chapter. We let f operate on ψ by applying the following operator to ψ.

$$a_{400}\frac{\partial}{\partial e_1^4} + 4a_{310}\frac{\partial}{\partial e_1^3 \partial e_2} + 6a_{220}\frac{\partial}{\partial e_1^2 \partial e_2^2} + \cdots + a_{004}\frac{\partial}{\partial e_3^4}.$$

The result is a covariant $S^4(V^*) \to S^2(V)$ of degree 4 and index 6. More precisely it is a contravariant, see Section 1.3. Hilbert ascribes this procedure to Clebsch, see (Shafarevich 1983).

5.2.3 Equivalence in $S^2(V)$

Applying the covariant that is explained in Subsection 5.2.2 allows us to first solve the equivalence problem in the space $S^2(V)$. There exists a normal form for $\mathrm{SL}(V)\colon S^2(V)$. To be precise, there is the following theorem, see for example (Kraft 1984) or (Broida and Williamson 1989). See also the example in Section 1.4, for the two-dimensional theorem for finite fields.

Theorem 27 *Let $f \in S^2(V)$ and let δ equal its discriminant. If $\delta \neq 0$ then there exists an $A \in \mathrm{SL}(V)$ such that $A \cdot f = \delta e_1^2 + e_2^2 + e_3^2$.*

Applying the discriminant after applying the covariant in Subsection 5.2.2 gives an invariant of degree 12. If this invariant is zero for both f_1 and f_2 then the algorithm as written here breaks down. We have to assume that this invariant evaluates to zero for at most one of f_1 and f_2. In the case that one is zero and the other is not, the forms f_1 and f_2 are not equivalent.

We compute $\mathrm{cov}(f_1)$ and $\mathrm{cov}(f_2)$. If the discriminants of these two forms are not equal then f_1 and f_2 are not equivalent. Therefore, we will assume that the discriminants are equal. In fact, we can assume that the discriminants are 1. For, if not we let the matrix

$$D = \begin{pmatrix} \frac{1}{\sqrt{\delta}} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

act on f_1 and f_2. Then $C(D \cdot f) = D \cdot C(f)$ has discriminant 1. Note that D is not an element of $\mathrm{SL}_3(\mathbb{C})$ but if we later find an A such that $ADf_1 = Df_2$ then also $D^{-1}ADf_1 = f_2$ and $D^{-1}AD$ has determinant 1, if A has.

We can now find elements A_1 and A_2 in $\mathrm{SL}_3(\mathbb{C})$ such that $A_1 \cdot f_1 = A_2 \cdot f_2 = e_1^2 + e_2^2 + e_3^2$. Algorithms for doing this are in most textbooks on linear algebra. One exposition is given in (Broida and Williamson 1989).

We can now restrict ourselves to those $B \in \mathrm{SL}_3(\mathbb{C})$ for which $B \cdot (e_1^2 + e_2^2 + e_3^2) = e_1^2 + e_2^2 + e_3^2$. We try to find a $B \in \mathrm{SO}_3(\mathbb{C})$ such that $BA_1f_1 = A_2f_2$. To see that this is sufficient, suppose we have an $A \in \mathrm{SL}_3(\mathbb{C})$ such that $Af_1 = f_2$; then $B = A_2AA_1^{-1}$ satisfies first of all $BA_1f_1 = A_2f_2$, and second, since

$$B \cdot (e_1^2 + e_2^2 + e_3^2) = B\,\mathrm{cov}(A_1f_1) = \mathrm{cov}(BA_1f_1) = \mathrm{cov}(A_2f_2) = (e_1^2 + e_2^2 + e_3^2),$$

this B stabilizes $(e_1^2 + e_2^2 + e_3^2)$.

Hence we will restrict ourselves from now on to the stabilizer of $(e_1^2 + e_2^2 + e_3^2)$ in $\mathrm{SL}_3(\mathbb{C})$, that is the group $\mathrm{SO}_3(\mathbb{C})$. This is a proper subgroup of $\mathrm{SL}_3(\mathbb{C})$ so this will make the problem easier.

5.2.4 A Surjective Homomorphism from $\mathbf{SL}_2$ to $\mathbf{SO}_3$

It turns out to be computationally convenient if an other quadratic form takes the place of $e_1^2 + e_2^2 + e_3^2$. Let

$$T = \begin{pmatrix} 0 & I/2 & 1/2 \\ 1 & 0 & 0 \\ 0 & I/2 & -1/2 \end{pmatrix},$$

where $I^2 = -1$. Then $T \cdot (e_1^2 + e_2^2 + e_3^2) = e_2^2 - e_1 e_3$. So $C(TA_1 \cdot f_1) = C(TA_2 \cdot f_2) = e_2^2 - e_1 e_3$. We can now restrict ourselves to the stabilizer of $e_2^2 - e_1 e_3$ in $\mathrm{SL}_3(\mathbb{C})$. This subgroup of $\mathrm{SL}_3(\mathbb{C})$ is isomorphic to $\mathrm{SO}_3(\mathbb{C})$ (since it leaves a non-degenerate quadratic form invariant). Again the determinant of T is not 1. But if we find an X such that $XTA_1 f_1 = TA_2 f_2$ then $A_2^{-1}T^{-1}XTA_1 f_1 = f_2$ and $A_2^{-1}T^{-1}XTA_1$ has determinant 1.

We are going to examine further the action of SO_3 on $S^4(V^*)$. Let X be a vector space isomorphic to $\mathbb{C}^2$. We will find two maps:

$$\begin{aligned} r\colon S^2(X^*) &\to V^* \\ s\colon \mathrm{SL}(X) &\to \mathrm{SO}_3(V) \end{aligned}$$

such that r is an isomorphism, s is a surjective morphism and satisfying $s(A) \cdot r(f) = r(A \cdot f)$ for all $A \in \mathrm{SL}(X)$ and all $f \in S^2(X^*)$. Let $\{a, b\}$ be a basis for X^*. Then $\{a^2, 2ab, b^2\}$ is a basis for $S^2(X^*)$. The linear mapping r is defined by

$$r(a^2) = x, \quad r(2ab) = y, \quad r(b^2) = z.$$

To satisfy the formula $s(A) \cdot r(f) = r(A \cdot f)$ we compute $r(A \cdot f)$ for f in the basis of $S^2(X^*)$ and a general element A of $\mathrm{SL}_2(\mathbb{C})$. We obtain the following mapping:

$$s\colon \begin{pmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{pmatrix} \mapsto \begin{pmatrix} s_{11}^2 & 2s_{11}s_{12} & s_{12}^2 \\ s_{11}s_{21} & s_{11}s_{22} + s_{21}s_{12} & s_{22}s_{12} \\ s_{21}^2 & 2s_{21}s_{22} & s_{22}^2 \end{pmatrix}.$$

Because $\mathrm{SL}_2(\mathbb{C})$ leaves the discriminant invariant, the image of $\mathrm{SL}_2(\mathbb{C})$ under s leaves $e_2^2 - e_1 e_3$ invariant. Hence the image of $\mathrm{SL}_2(\mathbb{C})$ lies in $\mathrm{SO}_3(\mathbb{C})$ and leaves the form invariant that we fixed above. The mapping s is a surjective 2 to 1 mapping.

At this point we are really examining the action of $\mathrm{SL}_2(\mathbb{C})$ on $S^4(S^2(X^*))$. We can see the above as the definition of an action of $\mathrm{SL}_2(\mathbb{C})$ on V. Using this view we can say that there exists an element $B \in \mathrm{SL}_2(\mathbb{C})$ such that $B \cdot (A_1 f_1) = A_2 f_2$ if and only if such an element in $\mathrm{SO}_3(\mathbb{C})$ exists.

5.2.5 Mapping to $S^4(X^*)$

Now we can view the action of SO_3 on $S^4(V^*)$ as an action of $\mathrm{SL}_2(\mathbb{C})$ on $S^4(V^*) = S^4(S^2(X^*))$. According to (Fulton and Harris 1991) or using the computer program LiE, see (van Leeuwen, Cohen, and Lisser 1992), the space $S^4(S^2(X^*))$ decomposes as:

$$S^4(S^2(X^*)) \cong S^8(X^*) + S^4(X^*) + S^0(X^*).$$

From this decomposition alone it is not possible to actually perform the mappings with concrete elements. It is only known that such a map exists. In Section 5.3 we will make this map explicit using Lie algebra theory. For now we will just assume that we have those results already.

To be precise, for the $\mathrm{SL}_2(\mathbb{C})$ action as described above, we use the following theorem.

Theorem 28 *There is a polynomial map $\alpha\colon S^4(V^*) \to S^4(X^*)$ such that*

$$\alpha(gf) = g\alpha(f),$$

for any $g \in \mathrm{SL}_2(\mathbb{C})$ and $f \in S^4(V^*)$.

Let us see how this theorem fits in. We have f_1 and f_2 and we want to know if there exists an $A \in \mathrm{SL}_3(\mathbb{C})$ such that $Af_1 = f_2$. In Subsection 5.2.3 we reduced this to finding an element $B \in \mathrm{SO}_3$ such that $BA_1f_1 = A_2f_2$. In turn this reduced to finding a $B \in \mathrm{SL}_2(\mathbb{C})$ such that $BA_1f_1 = A_2f_2$.

Using the above theorem we obtain the implication that if there exists such a B then there will also exist a B such that $B\alpha(A_1f_1) = \alpha(A_2f_2)$. The reverse implication need not necessarily be true, but at this point the number of possible $B \in \mathrm{SL}_2(\mathbb{C})$ that map the one form into the other has become small enough to make it feasible to check for all these B whether they also work for A_1f_1 and A_2f_2. To obtain the element that maps f_1 to f_2 we compute $A_2^{-1}s(B)A_1$.

We can now make precise the notation of regularity, from Theorem 25.

Definition 23 *A homogeneous polynomial f of degree 4 in 3 variables is called a* regular *quartic if the following conditions hold:*

(1) The discriminant of the quadratic form $\mathrm{cov}(f)$ is not zero, see Subsection 5.2.2.

(2) The binary quartic obtained from the algorithm in Subsection 5.2.5 does not have multiple zeros.

A few remarks on this definition. First of all the space of quartics that are not regular is Zariski closed with respect to the space of all quartics. Hence regular quartics are dense with respect to all quartics. Note also that the second condition cannot be certified unless the first step is already satisfied. To recognize a non-regular quartic one is essentially running the algorithm on one quartic instead of two.

5.2.6 Equivalence Problem in $S^4(X^*)$

As we have seen above, our equivalence problem reduces to solving the equivalence problem for binary polynomials of degree 4. This problem has two aspects: first of all, given two binary quartics we want to determine whether they are equivalent and secondly if they are equivalent, how can we transform one of them in the other. We will describe three approaches to this problem.

We find invariants for binary quartics. This is a solved problem so to complete this discussion we list the relevant invariants, found using the symbolic method from Chapter 3. They are:

$$\begin{aligned} [1,2]^4, \\ ([1,2][1,3][2,3])^2. \end{aligned} \tag{5.2}$$

The first is called the *apolar invariant*, the second is the Hankel invariant used in Subsection 5.2.2. For the binary quartic

$$a_{40}x^4 + a_{31}4x^3y + a_{22}6x^2y^2 + a_{13}4xy^3 + a_{04}y^4,$$

these invariants are equal to:

$$\begin{aligned} 2a_{40}a_{04} - 8a_{31}a_{13} + 6a_{22}^2, \\ 6a_{22}a_{04}a_{40} - 6a_{31}^2a_{04} + 12a_{31}a_{13}a_{22} - 6a_{40}a_{13}^2 - 6a_{22}^3. \end{aligned}$$

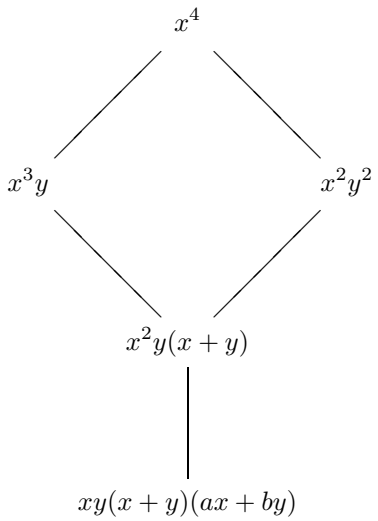
We compute them for $\alpha(A_1 f_1)$ and $\alpha(A_2 f_2)$. If they do not agree then the forms are not equivalent. On the other hand if they are equal and not zero then we need to find B such that $B\alpha(A_1 f_1) = \alpha(A_2 f_2)$. Finally if they are both zero then this approach breaks down. Both forms are in the null-cone. (The null-cone of $S^4(X^*)$ consists of quartics with a tripple zero.)

The second approach we could take is the following. There exists a normal form for binary quartics. One way to find such a normal form is to map three of its four roots to fixed positions. To do this we have to add a few forms for the degenerate cases.

In total there are five cases: four forms and one class of forms. Note that some of these forms are contained in the closure of the orbit generated by some other form. For example, x^4 is contained in the closure of the orbit of x^3y. This can be shown as follows: By using the $\mathrm{SL}_3(\mathbb{C})$ element

$$\begin{pmatrix} t & 1/t^3 \\ 0 & 1/t \end{pmatrix}$$

the form x^3y is equivalent to the form $x^4 + t^2x^3y$, for each $t \in \mathbb{R} \setminus \{0\}$. As t goes to zero, the latter will converge to x^4. The relationships between the forms is indicated in the diagram below. Each form is contained in the closure of the orbit generated by the form(s) below it.



To find out to which class a form is equivalent, you first find all its roots. Then if some of these roots are duplicated you know in which class it falls. And if they don't you can map the set of roots to the roots of the fourth curve. In the latter case you will need to consider all 4! permutations to get all possibilities. An advantage of this method is that it deals with the degenerate cases that can arise. A disadvantage is that it necessitates the computation of the roots of a degree 4 polynomial. Although this is possible it makes actual computations cumbersome since one must keep track of the often large expressions for the roots.

Finally the third way to look at it, is as follows. Just transform your form with a general element in $\mathrm{SL}_2(\mathbb{C})$. We obtain a set of equations on the coefficients by setting the transformed form equal to the target form. This gives 5 equations of degree 4 and 1 equation of degree 2 (expressing that the determinant is 1) in 4 unknowns. Then compute a Gröbner basis with respect to a lexicographic ordering and solve for the unknowns. This may be a rather crude approach since Gröbner basis computations are in general rather inefficient. However, in this particular case it worked rather well for the computations that we have tried. This is probably because the group $\mathrm{SL}_2(\mathbb{C})$ is small, it has only 3 free parameters.

All of these approaches have been implemented and tried for non-singular quartics. From a practical point of view it was easiest to first check equivalence using invariants and then find the transforming matrices using a Gröbner basis computation.

5.3 The Decomposition of $S^4(S^2(X^*))$

In this section we will construct the mapping

$$S^4(S^2(X^*)) \cong S^8(X^*) + S^4(X^*) + S^0(X^*)$$

that we needed in Subsection 5.2.5. Elements of $S^8(X^*) + S^4(X^*) + S^0(X^*)$ will be denoted by (f_1, f_2, f_3), where f_1, f_2 and f_3 are elements of $S^8(X^*)$, $S^4(X^*)$ and $S^0(X^*)$, respectively. Corresponding to the action of $\mathrm{SL}_2(\mathbb{C})$ there is an action of the Lie algebra $\mathfrak{sl}_2(\mathbb{C})$. The decomposition and the associated mapping when we view $S^4(V^*)$ as a $\mathrm{SL}_2(\mathbb{C})$ module are the same as when we consider is an $\mathfrak{sl}_2(\mathbb{C})$ module. We are going to compute the weight vectors of the Lie algebra module given by the action on $S^4(V^*)$ and then map those to the corresponding weight vectors of $S^8(X^*) + S^4(X^*) + S^0(X^*)$.

A representation of the Lie algebra $\mathfrak{sl}_2(\mathbb{C})$ acting on X^* is spanned by the following three elements:

$$e = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad f = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

In this section we will use the assignment $A = x^2$, $B = 2xy$ and $C = y^2$, thus A, B and C are a basis for $S^2(X^*)$. The action of e on V can now be computed. For example $\mathrm{ad}(e)A = \mathrm{ad}(e)x^2 = 2x(\mathrm{ad}(e)x) = 2x \cdot 0 = 0$. After all the necessary computations we find that e, f and h correspond to the following matrices: (We have in effect found a 3-dimensional representation of $\mathfrak{sl}_2(\mathbb{C})$.)

$$e \to \begin{pmatrix} 0 & 2 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad h \to \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -2 \end{pmatrix}, \quad f \to \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix}.$$

Note that the weights of this representation, that is the eigenvalues of h, are 2, 0 and -2, which is to be expected.

In this fashion we can also work out the weights that will occur on the right hand side. That is, the weights of $S^8(X^*)$, $S^4(X^*)$ and $S^0(X^*)$. We obtain

$$\begin{gathered} 8, 6, 4, 2, 0, -2, -4, -6, -8 \\ 4, 2, 0, -2, -4 \\ 0 \end{gathered}$$

We know that we can expect the same weights in the decomposition of $S^4(S^2(X^*))$.

Monomials like $A^i B^j C^k$ are eigenvectors of h, since

$$h \cdot (A^i B^j C^k) = (2i - 2k) A^i B^j C^k,$$

and hence these lie in weight spaces. We also know their weights. Since the number of these vectors (16) is the same as the dimension of the whole space we know we have all of the eigenvectors of h. In particular the element corresponding to weight 8 (the highest weight) is A^4, it is also a highest weight vector. Up to scalar multiples the weight 8 vectors are unique.

So we have to map A^4 to $(x^8, 0, 0)$. This pins down a large part of the mapping we are after. For we have to map $f \cdot A^4$ to $f \cdot (x^8, 0, 0)$, and the same goes for higher powers of f. Lie theory (see (Fulton and Harris 1991) for all Lie references) tells

us that in this way we get a complete set of 9 vectors with weights 8 to -8 (going down by 2) and their images. If v is a weight vector of weight λ then $f \cdot v$ is a weight vector of weight $\lambda - 2$ and $e \cdot v$ a weight vector of weight $\lambda + 2$.

There are two monomials of weight 4, A^3C and A^2B^2. Together they span a weight space. Since $f^2 \cdot A^4$ also has weight 4, it lies in this weight space. Also we know what its image should be; $f^2 \cdot A^4$ maps to $f^2 \cdot (x^8, 0, 0)$. In order to find the image of the whole of this weight space we compute a highest weight vector w with weight 4. This vector will map to $(0, x^4, 0)$, since it is also an irreducible space with highest weight 4. Such a vector w has the property that $e \cdot w = 0$. We obtain: $e \cdot (\alpha A^2B^2 + \beta A^3C) = \alpha 4A^3B + \beta A^3B$. So $w = A^2B^2 - 4A^3C$. Applying f to this gives us 5 more vectors and their images. We can determine a vector that maps to $(0, 0, 1)$. In the same manner as above we get: $e \cdot (\alpha A^2C^2 + \beta AB^2C + \gamma B^4) = (2\alpha + 4\beta)A^2BC + (\beta + 8\gamma)B^3A = 0$ hence $B^4 - 8AB^2C + 16A^2C^2$ maps to $(0, 0, 1)$.

5.4 An Example

This section serves as an example for the preceding sections. We are given two quartics:

$$\begin{aligned} f_1 &= x^4 + y^4 + z^4 + 6x^2y^2 - 12x^2yz, \\ f_2 &= 37541x^4 + 97z^4 + 17y^4 - 104y^3z \\ &\quad - 14268x^2yz + 3240xyz^2 - 2088xy^2z \\ &\quad - 33300x^3z + 240y^2z^2 - 248yz^3 + 452xy^3 \\ &\quad - 1692xz^3 + 11196x^2z^2 + 21176x^3y + 4590x^2y^2. \end{aligned}$$

First we compute the values of the covariant cov. The basis for the dual space is expressed here as $\{u, v, w\}$.

$$\begin{aligned} Cf_1 &= -576wv - 1152v^2 + 144u^2, \\ Cf_2 &= 1296w^2 + 288uv + 144u^2 - 7920v^2 - 7200wv + 1440uw. \end{aligned}$$

To find their normal form we will transform these with the following matrices:
First we transform Cf_1 to $u^2 + v^2 + w^2$ with the matrix:

$$\begin{pmatrix} \frac{1}{12} & 0 & 0 \\ 0 & -\frac{I\sqrt{2}}{48} & 0 \\ 0 & \frac{\sqrt{2}}{48} & -\frac{\sqrt{2}}{12} \end{pmatrix}.$$

Then multiplying this with

$$\begin{pmatrix} 0 & I/2 & 1/2 \\ 1 & 0 & 0 \\ 0 & I/2 & -1/2 \end{pmatrix}$$

will take Cf_1 to $v^2 - uw$. The matrix we get is

$$A_1 = \begin{pmatrix} 0 & \frac{\sqrt{2}}{48} & -\frac{\sqrt{2}}{24} \\ \frac{1}{12} & 0 & 0 \\ 0 & 0 & \frac{\sqrt{2}}{24} \end{pmatrix}.$$

Applying A_1 to f_1 (remembering to take the dual action, by inverting and transposing) we get the 'half normal' form

$$\begin{aligned} fn_1 = {} & 20736y^4 + 1327104x^4 + 5308416x^3z + 7962624x^2z^2 \\ & + 5308416xz^3 + 1410048z^4 + 995328x^2y^2 + 995328xy^2z. \end{aligned}$$

In a similar way we compute A_2

$$A_2 = \begin{pmatrix} \frac{31\sqrt{14}}{168} & \frac{\sqrt{14}}{42} & -\frac{\sqrt{14}}{24} \\ \frac{1}{12} & 0 & 0 \\ -\frac{3\sqrt{14}}{16} & -\frac{\sqrt{14}}{48} & \frac{\sqrt{14}}{24} \end{pmatrix}.$$

The half-normalized curve for f_2 is then

$$\begin{aligned} fn_2 = {} & 20736y^4 + 995328xy^2z + 21233664/7xz^3 + 7962624x^2z^2 \\ & + 1741824x^2y^2 + 9289728x^3z + 22560768/49z^4 + 4064256x^4. \end{aligned}$$

Next we are going to apply the mapping from $S^4(V^*)$ to $S^4(X^*)$. The results of transforming fn_1 to fs_1 and fn_2 to fs_2 are:

$$\begin{aligned} fs_1 &= -30855168/7x^4 - 64571904/7x^2y^2 - 31850496/7y^4, \\ fs_2 &= -7713792x^4 - 64571904/7x^2y^2 - 127401984/49y^4. \end{aligned}$$

Computing the invariants (5.2) for fs_1 and fs_2 gives these values :

$$\frac{1330213303812096}{49}, \qquad -\frac{9329909446831503310848}{343}$$

for both forms. Hence we know fs_1 and fs_2 are equivalent. To find a map between them we compute the roots of both fs_1 and fs_2. Luckily in this case these are forms in x^2 and y^2 so these roots are easy to compute. The following element from $\mathrm{SL}_2(\mathbb{C})$ takes fs_1 to fs_2

$$\begin{pmatrix} \frac{\sqrt{2}\sqrt[4]{7^3}}{7} & 0 \\ 0 & \frac{\sqrt{2}\sqrt[4]{7}}{2} \end{pmatrix}.$$

Mapping the latter to $\mathrm{SO}_3(\mathbb{C})$ gives us:

$$S = \begin{pmatrix} \frac{2\sqrt{7}}{7} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \frac{\sqrt{7}}{2} \end{pmatrix}.$$

To find the final transformation to move f_1 to f_2 we compute $A_2^{-1}SA_1$:

$$\begin{pmatrix} 1 & 0 & 0 \\ 1 & 2 & 3 \\ 5 & 1 & 2 \end{pmatrix}.$$

Chapter 6

Quintics

6.1 Introduction

We will extend the techniques that were used for quartics in Chapter 5 to other cases. Recall Lemma 3 from Chapter 1.

Lemma 9 *Let G be a group and let V and W be vector spaces on which G acts. Let $\phi\colon V \to W$ be a G-covariant mapping. Let $f, g \in V$ and put $T = \{A \in G \mid A \cdot f = g\}$ and $U = \{A \in G \mid A \cdot \phi(f) = \phi(g)\}$. Then $T \subset U$.*

The set U is empty or a coset of the stabilizer $\mathrm{Stab}_G(\phi(f)) = \{A \in G | A\phi(f) = \phi(f)\}$. So if $\mathrm{Stab}_G(\phi(f))$ is finite then we have the following algorithm for deciding the equivalence question. We exhaustively try for each element B in U, whether $B \cdot f = g$. In this case, solving the equivalence problem in V is as hard as solving the equivalence problem in W *plus* computing the stabilizer of a point in W.

Even in the case that $\mathrm{Stab}_G(\phi(f))$ is not finite it might be that this group is simpler to work with. For example, in Chapter 5 we applied Theorem 3 to the space $S^4(V^*)$ and $S^2(V)$.

We take the special case where $G = \mathrm{SL}_3(\mathbb{C})$. We will explicitly construct a covariant $\phi\colon S^5(V^*) \to S^3(V^*)$. In this case we know from Chapter 4, Theorem 22 that $\mathrm{Stab}_G(\phi(f))$ is finite if $\phi(f)$ is non-singular. As noted before, finding an element in $\mathrm{SL}_3(\mathbb{C})$ that transforms one cubic into another is in general not trivial. But in the case of cubics it is at least clear how to find such a transformation in principle.

The straightforward implementation will fail when $\mathrm{Stab}_G(\phi(f))$ is not finite and this could be the case if $\phi(f)$ is singular. Therefore we need to look a bit better when a cubic is singular. Recall that there exist two invariants for elliptic curves, S and T (see Subsection 4.2.1 and Theorem 20), that generate all the invariants for cubics. They are of degrees 4 and 6, respectively. An elliptic curve is singular, see (Silverman 1986)[pp. 50], if and only if $T^2 + 216S^3 = 0$. The form $T^2 + 216S^3$ is also an invariant, so if we compose this invariant with the covariant ϕ, we get an invariant for quintics of degree $3 \cdot 12 = 36$ that is zero if and only if the image of

ϕ is singular. We will call quintics for which ϕ gives a non-singular cubic, *regular quintics*. That means that the algorithm outlined in this chapter works for all quintics except those on a degree 36 hypersurface. We summarize the result in the following theorem.

Theorem 29 *Let f_1 and f_2 be two regular quintics defined over $\mathbb{C}$. There exists an algorithm that produces two cubics g_1 and g_2, such that f_1 and f_2 are equivalent if and only if there exists an $A \in \mathrm{SL}_3(\mathbb{C})$ such that $Ag_1 = g_2$ and $Af_1 = f_2$. Moreover, there are only finitely many A for which $Ag_1 = g_2$.*

Proof: Let $\phi\colon S^5(V^*) \to S^3(V^*)$ be the covariant that will be constructed in this chapter. Set $g_1 = \phi(f_1)$ and $g_2 = \phi(f_2)$. If f_1 and f_2 are equivalent, then there exists an $A \in \mathrm{SL}_3(\mathbb{C})$ such that $Af_1 = f_2$. By covariance this A also satisfies, $Ag_1 = g_2$. On the other hand ϕ satisfies the requirements of Lemma 3 from Chapter 1. By the regularity of the quintics, the cubics g_1 and g_2 are not singular and therefore the set $\{X \in \mathrm{SL}_3(\mathbb{C}) \mid Xg_1 = g_2\}$ is finite. □

6.2 Constructing the Covariant

We construct covariants in the following way. For any integer n, we map $S^5(V^*)$ with a covariant to $S^n(S^5(V^*))$ as in the example on Page 6.

The space $S^n(S^5(V^*))$ will, for most n, be reducible as an $\mathfrak{sl}_3(\mathbb{C})$ Lie algebra module. To decompose such a space, given n, we use the computer algebra package LiE (van Leeuwen, Cohen, and Lisser 1992). When we find an n for which the decomposition contains a space that is sufficiently simple for our purposes, we can use it to construct a covariant.

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

$$\begin{aligned} S^3(S^5(V^*)) = {} & \Gamma[0,3] + \Gamma[0,9] + \Gamma[0,15] + \Gamma[2,5] + \Gamma[2,11] \\ & + \Gamma[3,0] + \Gamma[3,3] + \Gamma[3,6] + \Gamma[3,9] + \Gamma[4,7] \\ & + \Gamma[5,2] + \Gamma[5,5] + \Gamma[6,3]. \end{aligned} \tag{6.1}$$

In this equation $\Gamma[a,b]$ denotes an $\mathrm{SL}_3(\mathbb{C})$-invariant subspace with highest weight vector (a,b), see Subsection 2.4.2. Of interest in this decomposition is the occurrence of $\Gamma[0,3]$. This is a subspace isomorphic to $S^3(V^*)$. The covariant is constructed as follows. Suppose we are given a quintic f for which we want to compute the value of the covariant. First compute $S^3(f)$, the third symmetric tensor power of f; this gives an element in $S^3(S^5(V^*))$. Next we map this element to $S^3(V^*)$. On a computer the first step might be performed as follows. Number all the monomials in $S^5(V^*)$, there are 21 of them, say we label them c_1 to c_{21}. Then write f as a linear combination of the monomials $c_1, \ldots c_{21}$. We now need only compute f^3. It is a priori possible that the set $\{S^3(f) \mid f \in S^5(V^*)\}$ might not intersect the irreducible subspace that we are interested in. So it is necessary to check, after we have constructed the desired covariant, that there exists at least one f for which it

is not zero. Once we know that, we also know that there must be a trivial kernel, otherwise the space $S^5(V^*)$ would not be irreducible.

Apart from this last consideration, we have basically proved the existence of a covariant $\phi\colon S^5(V^*) \to S^3(V^*)$ of degree 3. We can try to construct it using Lie theory, as we did in Subsection 5.2.4. Unfortunately the space $S^3(S^5(V^*))$ is a bit large. To be precise, the space $S^5(V^*)$ has dimension $\binom{5+2}{2} = 21$ and hence the space $S^3(S^5(V^*))$ has dimension $\binom{3+20}{20} = 1771$. If needed, it would probably be possible to construct the map in the straightforward manner, especially if enough computer power is spent on such a project. In the rest of this chapter we will show how the covariant can be described much more efficiently using the Casimir operator. First we will have to find the highest weight vectors of the Lie algebra representation that is induced by the action of $\mathrm{SL}_3(\mathbb{C})$ on $S^3(S^5(V^*))$.

6.2.1 Highest Weight Vectors in $S^3(S^5(V^*))$

We are studying the representation of $\mathfrak{sl}_3(\mathbb{C})$ on $S^3(S^5(V^*))$. We will view the algebra $\mathfrak{sl}_3(\mathbb{C})$ in its natural representation on V, and spanned by the following usual basis elements. Let $E_{i,j}$ be the 3×3 matrix that is everywhere zero except at (i, j) where it is 1. Let the Cartan subalgebra $\mathfrak{h}$ be spanned by

$$h_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad h_2 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

We need the following characterization of a highest weight vector of $\mathfrak{sl}_3(\mathbb{C})$, (see Section 2.4.2 and (Fulton and Harris 1991, p. 167).)

Lemma 10 *There is an eigenvector $v \in S^3(S^5(V^*))$ of $\mathfrak{h}$, such that v is killed by $E_{1,2}$, $E_{1,3}$ and $E_{2,3}$.*

To find all the highest weights we perform the following operations:

(1) Make a list of all 1771 monomials in $S^3(S^5(V^*))$ and calculate their weights (these are the eigenvectors of $\mathfrak{h}$).

(2) For each weight given in Decomposition (6.1) find all monomials with the same weight.

(3) Write down a general linear combination with these monomials and apply Lemma 10.

(4) Solve the linear equations produced by the last step.

The resulting list of highest weight vectors is given in a table. For clarity, elements from the space $S^5(V^*)$ are written between square brackets.

$\Gamma[15,0]$ $[x^5]^3$

$\Gamma[11,2]$ $[x^5]^2[x^3y^2] - [x^5][x^4y]^2$

$\Gamma[9,3]$ $[x^5]^2[x^2y^3] - 3[x^5][x^4y][x^3y^2] + 2[x^4y]^3$

$\Gamma[9,0]$ $-[x^5][x^3y^2][x^3z^2] + [x^5][x^3yz]^2 + [x^4y]^2[x^3z^2] - 2[x^4y][x^4z][x^3yz] + [x^4z]^2[x^3y^2]$

$\Gamma[7,4]$ $[x^5]^2[xy^4] - 4[x^5][x^4y][x^2y^3] + 3[x^5][x^3y^2]^2$

$\Gamma[6,3]$ $-[x^5][x^3y^2][x^2y^2z] + [x^5][x^3yz][x^2y^3] + [x^4y]^2[x^2y^2z] - [x^4y][x^4z][x^2y^3] - [x^4y][x^3y^2][x^3yz] + [x^4z][x^3y^2]^2$

$\Gamma[5,5]$ $[x^5]^2[y^5] - 5[x^5][x^4y][xy^4] + 2[x^5][x^3y^2][x^2y^3] + 8[x^4y]^2[x^2y^3] - 6[x^4y][x^3y^2]^2$

$\Gamma[5,2]$ $-[x^2yz^2][x^5][x^2y^3] + [x^2yz^2][x^4y][x^3y^2] + [x^5][x^3y^2][xy^2z^2] - 2[x^5][x^3yz][xy^3z] + [x^5][x^3z^2][xy^4] + [x^5][x^2y^2z]^2 - [x^4y]^2[xy^2z^2] + 2[x^4y][x^4z][xy^3z] + 2[x^4y][x^3yz][x^2y^2z] - 3[x^4y][x^3z^2][x^2y^3] - [x^4z]^2[xy^4] - 4[x^4z][x^3y^2][x^2y^2z] + 4[x^4z][x^3yz][x^2y^3] + 2[x^3y^2]^2[x^3z^2] - 2[x^3y^2][x^3yz]^2$

$\Gamma[3,6]$ $-[x^5][x^3y^2][xy^4] + [x^5][x^2y^3]^2 + [x^4y]^2[xy^4] - 2[x^4y][x^3y^2][x^2y^3] + [x^3y^2]^3$

$\Gamma[3,3]$ $-3[x^2yz^2][x^5][xy^4] + 18[x^2yz^2][x^4y][x^2y^3] - 15[x^2yz^2][x^3y^2]^2 + 2[x^5][x^3y^2][y^3z^2] - 4[x^5][x^3yz][y^4z] + 2[x^5][x^3z^2][y^5] - 3[x^5][x^2y^3][xy^2z^2] + 6[x^5][x^2y^2z][xy^3z] - 2[x^4y]^2[y^3z^2] + 4[x^4y][x^4z][y^4z] + 3[x^4y][x^3y^2][xy^2z^2] + 4[x^4y][x^3yz][xy^3z] - 7[x^4y][x^3z^2][xy^4] - 18[x^4y][x^2y^2z]^2 - 2[x^4z]^2[y^5] - 10[x^4z][x^3y^2][xy^3z] + 10[x^4z][x^3yz][xy^4] + 30[x^3y^2][x^3yz][x^2y^2z] + 5[x^3y^2][x^3z^2][x^2y^3] - 20[x^3yz]^2[x^2y^3]$

$\Gamma[3,0]$ $-12[x^2yz^2][x^4y][xy^2z^2] + 12[x^3z^2][x^2y^2z]^2 + 3[x^3z^2]^2[xy^4] + 12[x^3yz]^2[xy^2z^2] + 3[x^3y^2]^2[xz^4] + 3[x^5][xy^2z^2]^2 + 12[x^2yz^2]^2[x^3y^2] + 12[x^2yz^2][x^4z][xy^3z] - 12[x^2yz^2][x^3yz][x^2y^2z] + 12[x^3yz][x^2y^3][x^2z^3] - 12[x^3y^2][x^2y^2z][x^2z^3] - 12[x^3yz][x^3z^2][xy^3z] - 4[x^4z][x^2z^3][xy^4] - 12[x^3y^2][x^3yz][xyz^3] + 6[x^3y^2][x^3z^2][xy^2z^2] + 4[x^4z][x^2y^3][xyz^3] - 12[x^4z][x^2y^2z][xy^2z^2] - 4[x^4y][x^2y^3][xz^4] + 12[x^4y][x^2y^2z][xyz^3] + 4[x^4y][x^2z^3][xy^3z] - 12[x^2yz^2][x^3z^2][x^2y^3] + [x^5][xy^4][xz^4] - 4[x^5][xy^3z][xyz^3]$

$\Gamma[2,5]$ $[x^5][x^3y^2][y^4z] - [x^5][x^3yz][y^5] - 2[x^5][x^2y^3][xy^3z] + 2[x^5][x^2y^2z][xy^4] - [x^4y]^2[y^4z] + [x^4y][x^4z][y^5] + 2[x^4y][x^3y^2][xy^3z] + [x^4y][x^3yz][xy^4] - 2[x^4y][x^2y^3][x^2y^2z] - 3[x^4z][x^3y^2][xy^4] + 2[x^4z][x^2y^3]^2$

$\Gamma[0,3]$ $3[x^2y^3]^2[x^2z^3] + 6[x^4z][xy^3z]^2 + 6[x^3yz]^2[y^4z] + 3[x^3y^2]^2[y^2z^3] - 2[x^3y^2][x^2y^3][xyz^3] + 3[x^4y][xy^4][xyz^3] - 9[x^2yz^2][x^2y^3][x^2y^2z] + 9[x^3z^2][x^2y^2z][xy^4] - 3[x^2yz^2][x^3yz][xy^4] - 4[x^3y^2][x^2z^3][xy^4] - 9[x^3z^2][x^2y^3][xy^3z] - 12[x^3yz][x^2y^2z][xy^3z] + 15[x^2yz^2][x^3y^2][xy^3z] + 15[x^3yz][x^2y^3][xy^2z^2] - 9[x^3y^2][x^2y^2z][xy^2z^2] - 6[x^4z][xy^4][xy^2z^2] - 3[x^4y][xy^3z][xy^2z^2] + 6[x^2y^2z]^3 - [x^5][xyz^3][y^5] + 3[x^2yz^2][x^4z][y^5] + [x^4y][x^2z^3][y^5] - 3[x^3yz][x^3z^2][y^5] - 6[x^4z][x^2y^2z][y^4z] - 6[x^2yz^2][x^4y][y^4z] + 3[x^5][xy^2z^2][y^4z] + 3[x^3y^2][x^3z^2][y^4z] + 9[x^4y][x^2y^2z][y^3z^2] - 3[x^5][xy^3z][y^3z^2] - 9[x^3y^2][x^3yz][y^3z^2] + 3[x^4z][x^2y^3][y^3z^2] + [x^5][xy^4][y^2z^3] - 4[x^4y][x^2y^3][y^2z^3]$

6.2.2 The Casimir Operator

The Casimir operator is defined in Section 2.5. We take the standard basis E_{ij}, H_1, H_2 as the basis for $\mathfrak{sl}_3(\mathbb{C})$. Then the Casimir operator equals

$$\begin{aligned} C = {} & E_{12}E_{21} + E_{13}E_{31} + E_{23}E_{32} + E_{21}E_{12} + E_{32}E_{23} + E_{31}E_{13} \\ & + H_1(\frac{2}{3}H_1 + \frac{1}{3}H_2) + H_2(\frac{1}{3}H_1 + \frac{2}{3}H_2). \end{aligned}$$

We proceed as follows. For each of the highest weight vectors that we have found, we compute the scalar with which C multiplies it. If the eigenvalue of C for a particular irreducible subspace is μ then $C - \mu I$ projects this space onto 0. Ideally we would like to use C in this way to map each irreducible subspace of $S^3(S^5(V^*))$ to 0, *except* for the subspace $S^3(V^*)$. The latter space would only be multiplied with a constant in the process. This is possible if the eigenvalues of the irreducible subspace other than $S^3(V^*)$ would be unequal to the eigenvalue of $S^3(V^*)$.

It turns out that this is nearly the case. Only the eigenvalue for C of the irreducible subspace $S^3(V)$ is equal to the eigenvalue of $S^3(V^*)$.

Applying $C - \mu I$ for each of the occurring eigenvalues μ different from the eigenvalue of $S^3(V^*)$ maps $S^3(S^5(V^*))$ to $S^3(V) \oplus S^3(V^*)$. The dimension of $S^3(V) \oplus S^3(V^*)$ is only 20. To separate the remaining two irreducible subspaces we proceed as in the last part of Chapter 5. By applying the elements of $\mathfrak{sl}_3(\mathbb{C})$ to the two highest weights of these two irreducible spaces we get a basis for each of these spaces. Basic linear algebra can now tell how to map these spaces to each other.

Finally we need to check that there is a form that does not map to zero. The following quintic

$$\begin{aligned} x^5 + x^4y + x^4z + x^3y^2 + x^3yz + x^3z^2 + x^2y^3 + x^2y^2z + x^2yz^2 + x^2z^3 + \cdots \\ \cdots + xy^4 + xy^3z + xy^2z^2 + xyz^3 + xz^4 + y^5 \end{aligned}$$

maps to the form

$$-\frac{5}{14}z^2y - \frac{2}{7}zy^2 - \frac{1}{21}y^3 - \frac{9}{140}xz^2 - \frac{53}{70}xyz - \frac{9}{140}xy^2 - \frac{4}{35}zx^2 + \frac{67}{70}x^2y + \frac{3}{20}x^3,$$

the latter of which indeed is not zero (and in fact not singular). This procedure for mapping quintics to cubics is the covariant needed in Theorem 29.

Evaluating the covariant in this way, makes it necessary to compute the Casimir operator nine times, this will take a few seconds to evaluate. Alternatively, it is possible to precompute the value of the covariant for all the values in $S^3(S^5(V^*))$ and store them in a 1771×10 matrix. This matrix turned out to be sparse, making this approach fast. The precomputation took about a day of computing though.

6.3 Beyond

Whether one can use the method of this chapter in other cases depends on the availability of a suitable covariant. Experimenting with LiE led to the following conjecture. Let n, k be positive integers with $n \geq k$ and $k > 2$. Let $V = \mathbb{C}^k$. There is a non-trivial $\mathrm{SL}_k(\mathbb{C})$ covariant mapping

$$S^k(S^n(V^*)) \to \begin{cases} S^k(V^*) & \text{if } n \text{ is odd,} \\ S^0(V^*) & \text{if } n \text{ is even.} \end{cases}$$

The case n is even can be proven with the symbolic method; in fact it is the symbolic form given in Theorem 16 on Page 35. The other case was checked for:

$$\begin{aligned} k &= 3 \quad n \leq 35, \\ k &= 4 \quad n \leq 12, \\ k &= 5 \quad n \leq 9. \end{aligned}$$

Appendix A

Maple Implementations

The algorithms in this appendix were implemented using the computer algebra package *Maple V Release 5.1*. The list below is a selection of the essential algorithms discussed in this thesis. Most of the procedures listed are implemented by use of various others that perform subtasks.

Chapter 3

- The procedure $umbral(n, m, d, B)$ evaluates a bracket polynomial B with the umbral operator (see Section 3.3). B is a bracket polynomial. It is written as a list of lists, the latter contains a row each. The bracket polynomial B must satisfy the parameters n, m and d (see Section 3.3). The procedure uses Algorithm 2 from Subsection 3.4.1.

- The procedure $umbralway(n, m, d, B, A)$ evaluates a bracket polynomial for a specific given form only. The input A is an array containing the coefficients of the form. The procedure uses Algorithm 3 from Subsection 3.4.1.

Chapter 4

- The procedures $Sinv(f)$ and $Tinv(f)$ give the evaluation of the two invariants of degree 4 and 6 for cubics. f is a polynomial in x, y and z of degree 3. These procedures use the description based on contractions of tensor products, see (Popov and Vinberg 1994)[pp. 145].

- The procedure $galoisc(f, x)$ approximates the cycle-type distribution of the Galois group of a form f in the variable x. It uses the algorithm given in (Dummit and Foote 1991)[pp. 555].

Chapter 5

The equivalence algorithm is based on the following two procedures:

- The procedure *Cv*(coefficients of f) implements the covariant given in Subsection 5.2.2.
- The procedure *afb2s4*(f) maps a ternary quartic f on which $\mathrm{SO}_3(\mathbb{C})$ acts to a binary quartics on which $\mathrm{SL}_2(\mathbb{C})$ acts. See Subsection 5.2.5.

Chapter 6

- The procedure *Casimir*(f) computes the result of the Casimir operator on the ternary quintic f.
- The procedure *maps3s5*(f) maps a quintic f to a cubic. It uses the algorithm of Section 6.2. Various other procedures are used for finding and using the highest weight vectors of $S^3(S^5(V^*))$.

References

Bix, R. (1998). *Conics and cubics*. New York: Springer-Verlag. A concrete introduction to algebraic curves.

Blichfeldt, H. F. (1917). *Finite Collineation Groups*. The University of Chicago Press.

Bourbaki, N. (1981). *Groupes et algèbres de Lie, Chapitre 4, 5 et 6*. Éléments de Mathématique. Masson, Paris.

Brieskorn, E. and H. Knörrer (1986). *Plane algebraic curves*. Birkhäuser Verlag, Basel. Translated from the German by John Stillwell.

Broida, J. G. and S. G. Williamson (1989). *A Comprehensive introduction to linear algebra*. Addison-Wesley Publishing Company.

Cox, D., J. Little, and D. O'Shea (1997). *Ideals, varieties, and algorithms* (Second ed.). New York: Springer-Verlag. An introduction to computational algebraic geometry and commutative algebra.

de Concini, C. and C. Procesi (1976). A characteristic free approach to invariant theory. *Advances in Math. 21*(3), 330–354.

de Graaf, W. A. (2000). *Lie algebras: theory and algorithms*. Amsterdam: North-Holland Publishing Co.

Derksen, H. (1999). Polynomial bounds for rings of invariants. preprint.

Dixmier, J. (1987). On the projective invariants of quartic plane curves. *Adv. in Math. 64*(3), 279–304.

Dolgachev, I. V. (1994). *Introduction to geometric invariant theory*. Seoul: Seoul National University Research Institute of Mathematics Global Analysis Research Center.

Dummit, D. and R. Foote (1991). *Abstract Algebra*. Prentice-Hall.

Faber, C. (1990). Chow rings of moduli spaces of curves. I: The chow ring of $\bar{\mathcal{M}}_3$. *Ann. Math., II 132*(2), 331–319.

Feit, W. (1982). *The representation theory of finite groups*. North-Holland Publishing Company.

Fulton, W. (1969). *Algebraic curves. An introduction to algebraic geometry*. W. A. Benjamin, Inc., New York-Amsterdam. Notes written with the collaboration of Richard Weiss, Mathematics Lecture Notes Series.

Fulton, W. and J. Harris (1991). *Representation theory*. Springer-Verlag, New York. A first course, Readings in Mathematics.

Goodman, R. and N. R. Wallach (1998). *Representations and invariants of the classical groups*, Volume 68 of *Encyclopedia of mathematics and its applications*. Cambridge: Cambridge University Press.

Gordan, P. (1885, 1887, reprint: 1987). *Vorlesungen über Invariantentheorie* (Second ed.). New York: Chelsea Publishing Co. Erster Band: Determinanten. Zweiter Band: Binäre Formen. Edited by Georg Kerschensteiner.

Grosshans, F. D., G.-C. Rota, and J. A. Stein (1987). *Invariant theory and superalgebras*. Published for the Conference Board of the Mathematical Sciences, Washington, D.C.

Guillemin, V. and A. Pollack (1974). *Differential topology*. Englewood Cliffs, N.J.: Prentice-Hall Inc.

Gurevich, G. B. (1964). *Foundations of the theory of algebraic invariants*. Groningen: P. Noordhoff Ltd. Translated by J. R. M. Radok and A. J. M. Spencer.

Howe, R. (1983). Very basic Lie theory. *Amer. Math. Monthly 90*(9), 600–623.

Howe, R. (1984). Correction to: "Very basic Lie theory". *Amer. Math. Monthly 91*(4), 247.

Husemöller, D. (1987). *Elliptic Curves*. Number 111 in Graduate texts in mathematics. Springer-Verlag.

Jacobson, N. (1979). *Lie algebras*. New York: Dover Publications Inc. Republication of the 1962 original.

Katz, N. M. and B. Mazur (1985). *Arithmetic moduli of elliptic curves*. Annals of Mathematics Studies, No.108. Princeton University Press.

Kirwan, F. (1992). *Complex Algebraic Curves*. Number 23 in Student Texts. London Mathematical Society.

Kraft, H. (1984). *Geometrische methoden in der Invariantentheorie*. Aspekte der Mathematik. Vieweg.

Lang, S. (1965). *Algebra*. Addison-Weseley Publishing Company inc.

Mayr, E. W. and A. R. Meyer (1982). The complexity of the word problems for commutative semigroups and polynomial ideals. *Adv. in Math. 46*(3), 305–329.

Milnor, J. W. (1965). *Topology from the differentiable viewpoint*. The University Press of Virginia, Charlottesville, Va. Based on notes by David W. Weaver.

O'Connor, J. and E. Robertson. History of mathematics. `http://www-groups.dcs.st-and.ac.uk/~history/`.

Popov, V. L. and È. B. Vinberg (1994). *Invariant Theory*, Volume 55, Part II of *Encyclopedia of Mathematical Sciences*. Springer-Verlag. Translated by G.A. Kandall from the Russian edition that appeared in 1989 and was published by VINITI.

Procesi, C. (1982). *A primer of invariant theory*, Volume 1 of *Brandeis Lecture notes*. Notes taken by Giandomenico Boffi.

Rota, G.-C. (1999). Two turning points in invariant theory. *Math. Intelligencer 21*(1), 20–27.

Salmon, G. (1862). *A treatise on the analytic geometry of three dimensions. Vol. II*. New York: Chelsea Publishing Co. Fifth edition. Edited by Reginald A. P. Rogers, reprinted in 1965.

Salmon, G. (1877). *Vorlesungen über die Algebra der linearen Transformationen*. B.G. Teubner, Leipzig.

Salmon, G. (1879). *A treatise on the higher plane curves*. Chelsea Publising Company. a reprint was published in 1960.

Serre, J.-P. (1987). *Complex Semisimple Lie Algebras*. Springer-Verlag.

Serre, J.-P. (1997). *Galois cohomology*. Springer-Verlag, Berlin. Translated from the French by Patrick Ion and revised by the author.

Shafarevich, I. R. (1983). Zum 150. Geburtstag von Alfred Clebsch. *Math. Ann. 266*(2), 135–140.

Shioda, T. (1967). On the graded ring of invariants of binary octavics. *Amer. J. Math. 89*, 1022–1046.

Silverman, J. H. (1986). *The Arithmetic of Elliptic Curves*. Springer-Verlag.

Springer, T. A. (1977). *Invariant Theory*, Volume 585 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin-New York.

Steinberg, R. (1964). Differential equations invariant under finite reflection groups. *Trans. Amer. Math. Soc. 112*, 392–400.

Stewart, I. (1973, 1989). *Galois Theory* (Second. ed.). Chapman & Hall.

Sturmfels, B. (1993). *Algorithms in invariant theory*. Vienna: Springer-Verlag.

The GAP Group (1999). *GAP–Groups, Algorithms, and Programming, Version 4.1*. Aachen, St Andrews: The GAP Group. (`http://www-gap.dcs.st-and.ac.uk/~gap`).

van Leeuwen, M. A. A., A. M. Cohen, and B. Lisser (1992). *LiE, A package for Lie group computations*. Computer Algebra Nederland.

van Lint, J. H. and R. M. Wilson (1992). *A course in combinatorics*. Cambridge: Cambridge University Press.

Weyl, H. (1946). *The Classical Groups. Their Invariants and Representations* (Second ed.). Princeton, N.J.: Princeton University Press.

Index

action, 3
    on dual, 4
    on polynomials, 5
apolar invariant, 64

bracket, 24
    monomial, 24
        standard, 25
    polynomial, 24
    ring, 24

Cartan subalgebra, 15
Casimir operator, 17
cobounding, 51
cocycle, 51
cohomologous, 51
cohomology set, 51
contravariants, 6
covariant, 6
cubic, 43

diagonal action, 6

equivalence problem, 3
Euler identity, 5

first fundamental theorem, 25

Gröbner basis, 58
Grassmann-Plücker relation, 25
group
    Lie, 11
    topological, 11

Hankel determinant, 60
Hessian
    normal form, 43
    subspace, 43
highest weight, 16
Hilbert-Mumford Criterion, 19

ideal of syzygies, 25
inflection points, 43
invariant, 6
    index, 27

Lie algebra, 12

monomial, 5
multiplicity, 19

null-cone, 19, 57

orbit, 8

polynomials, 5

quintics
    regular, 72

regular, 63
representation of a Lie algebra, 13
root spaces, 15
roots, 15

second fundamental theorem, 25
semisimple, 14
stabilizer
    affine, 48
    projective, 49
support, 19
symbol, 24
symbolic method, 23

tableau, 24

standard, 25
tangent lines, 19

umbral operator, 26

Weierstrass section, 58
weight, 16

Dankbetuiging

Vier jaar lang ben ik uitstekend begeleid, geadviseerd en gesteund. Zonder die hulp zou het schrijven van dit proefschrift niet alleen veel zwaarder, maar ook een stuk minder leuk zijn geworden. Veel vrienden en collega's hebben mij op verschillende manieren geholpen. Er zijn een aantal mensen die ik graag met name wil bedanken.

Arjeh Cohen, begeleiding van je aio's kwam bij jou altijd op de eerste plaats. Als ik een beroep op je deed kon je altijd je agenda verschuiven. Jouw inbreng zorgde overal voor meer wiskundige inhoud. Bij elk onderwerp vond je altijd nieuwe richtingen om in te slaan.

Hans Sterk, heel veel uren heb je geluisterd naar mijn moeilijkheden en soms ook vooruitgang. Die gesprekken zijn voor mij heel waardevol geweest. Of het nu ging om algebraïsche meetkunde of om kinderverzorging, je adviezen waren voor een beginner als ik van onschatbare waarde.

Harm Derksen, helaas hebben we elkaar de afgelopen vier jaar niet veel kunnen zien. Desalniettemin liggen de ideeën die je met mij deelde aan de basis van hoofdstuk 5.

Ik dank de leden van de kleine commissie: A.E. Brouwer, A. Blokhuis en M. van der Put.

Saskia, je hebt het hele proefschrift van kaft tot kaft gelezen. Niet alleen is het Engels daardoor verbeterd, bij elk haakje openen staat nu ook een bijpassend haakje sluiten. Jij bleef me altijd motiveren en daarvoor ben ik je zeer erkentelijk.

Ik dank NWO voor hun financiering en organisatie; dit promotieonderzoek vond plaats binnen het NWO aandachtsgebied: 'Algoritmen in de algebra'.

Samenvatting

We kunnen de groep $\mathrm{SL}_3(\mathbb{C})$ laten werken op homogene polynomen in drie variabelen door middel van substitutie. Wanneer twee polynomen op deze manier in elkaar zijn over te voeren dan noemen we ze equivalent. In dit proefschrift wordt voornamelijk onderzoek gedaan naar algoritmen die over deze equivalentie uitspraak kunnen doen. Hierbij ligt de nadruk op effectieve methoden die daadwerkelijk op computers zouden kunnen worden toegepast. Er zijn twee aspecten te onderscheiden aan dit probleem. Enerzijds is er het beslissingsprobleem: zijn twee krommen wel of niet equivalent. Aan de andere kant is er het constructieprobleem: vind daadwerkelijk een element van $\mathrm{SL}_3(\mathbb{C})$ die de equivalentie aantoont. Het is duidelijk dat het tweede probleem minstens zo moeilijk is als het eerste.

De klassieke methode om het beslissingsprobleem aan te pakken is met behulp van invarianten. Wanneer een invariant voor twee krommen verschillende waarden aanneemt, dan zijn zij zeker niet equivalent. Het vinden van invarianten kan onder meer gebeuren met behulp van de symbolische methoden. We hebben onderzoek gedaan in hoeverre dit invarianten kan opleveren. Bovendien is er aandacht voor de vraag hoe deze symbolische expressies efficiënt kunnen worden geëvalueerd.

Voor ternaire polynomen, homogeen van graad 4, is het slechts mogelijk een relatief klein deel te vinden van de invarianten die nodig zijn om met zekerheid een uitspraak te doen over equivalentie. Bovendien kan met behulp van invarianten weinig vooruitgang geboekt worden voor het constructieprobleem. Voor dit geval hebben we gekeken naar een geheel andere methode. Deze werkt als volgt: Gegeven twee ternaire polynomen homogeen van graad 4, f_1 en f_2. Met behulp van een covariant worden deze afgebeeld op kwadrieken. Deze laatste kunnen we testen op equivalentie. Indien ze inderdaad equivalent zijn, dan is er een element A uit $\mathrm{SL}_3(\mathbb{C})$ zodat Af_1 en f_2 door bovengenoemde covariant naar hetzelfde element zouden worden afgebeeld. De deelgroep van $\mathrm{SL}_3(\mathbb{C})$ die deze kwadriek vasthoudt is isomorf met $\mathrm{SO}_3(\mathbb{C})$. De actie van $\mathrm{SO}_3(\mathbb{C})$ op vierdegraads polynomen in drie variabelen kan vervolgens worden getransformeerd naar een situatie waarin $\mathrm{SL}_2(\mathbb{C})$ werkt op vierdegraads polynomen in twee variabelen. Deze laatste situatie is veel beter bekend, hiervoor kan het equivalentieprobleem dan ook worden opgelost. Dit resulteert in een algoritme dat het equivalentieprobleem kan oplossen voor een klasse die dicht ligt.

De methode die werkt voor vierdegraads polynomen kan worden aangepast voor

krommen van de vijfde graad. Uit de decompositie van een bepaalde Lie algebra blijkt dat er een covariant moet bestaan die vijfdegraads krommen kan afbeelden naar derdegraads krommen. De constructie van een element van $\mathrm{SL}_3(\mathbb{C})$ die de equivalentie van twee vijfdegraads krommen kan aantonen is hiermee even complex geworden als het vinden van die elementen voor derdegraads krommen. Deze covariant is geconstrueerd door gebruik te maken van de Casimir operator. De afbeelding die reductie van vijfdegraads polynomen mogelijk maakt blijkt ook te bestaan voor krommen van andere graden. Er wordt gespeculeerd op mogelijk extensies van het algoritme.

Curriculum Vitae

Sander van Rijnswou werd geboren op 7 januari 1973 in Delft. In 1991 behaalde hij het diploma Atheneum aan het Christelijk Lyceum Delft. Van 1991 tot 1996 studeerde hij Technische Wiskunde aan de Technische Universiteit Delft, waar hij in 1996 cum laude afstudeerde in de richting algebra bij prof.dr.ir. Th.H.M. Smits met de scriptie 'On Schur Rings and Association Schemes'.

Van 1996 tot 2000 was Sander als OIO werkzaam bij NWO in het kader van het aandachtsgebied 'Algoritmen in de algebra' (AIDA) binnen de onderzoeksschool 'Euler Institute for Discrete Mathematics and its Applications' (EIDMA). Hij deed onderzoek naar mogelijkheden om vlakke krommen op equivalentie te testen. De nadruk lag hierbij op methoden die op een computer toepasbaar zijn.