Reconstruction of binary quintics

Noordsij, Jesper

J.G.I. Noordsij

Reconstruction of binary quintics

Master's thesis

Supervisor: dr. Marco Streng

Date master exam: January 24, 2022

Mathematical Institute,
Leiden University

Contents

Introduction

Invariant theory

Invariant theory is the study of invariants of homogeneous polynomials, which has a long history and still has many applications in modern mathematics. This thesis considers binary quintics, homogeneous polynomials of degree 5 with 2 variables, and the reconstruction of these objects from the values of their invariants. Moreover, the implementation of these invariants and the reconstruction in SageMath [Sage], a free open-source mathematics software system that can be used for these computations, is part of this thesis.

In the 19th century invariant theory was one of the main research topics in mathematics. Alfred Clebsch and Paul Gordan were among the ones trying to explicitly calculate invariants of so-called *(algebraic) forms*, which are simply homogeneous polynomials. This thesis will be mainly about binary quintic forms, where the word binary refers to the number of variables of the form, i.e. it has two variables, and the word quintic is connected to the degree, i.e. the form is of degree 5.

Perhaps the best known example of an *invariant* is the discriminant of a binary quadratic: given a polynomial $aX^2 + bXY + cY^2$, its discriminant is given by $b^2 - 4ac$. If one applies a linear transformation to the coordinates X and Y, i.e. one lets $X' = \alpha X + \beta Y$ and $Y' = \gamma X + \delta Y$ for some $\alpha, \beta, \gamma, \delta$ such that $\alpha\delta - \beta\gamma \neq 0$, then the discriminant of the resulting form is 'almost the same'. To be exact, the discriminant of the resulting form will be $(\alpha\delta - \beta\gamma)^2$ times the original discriminant, hence the discriminant is in some sense invariant under this operation.

This concept can be generalised to forms of different degrees or different numbers of variables. For binary forms, the discriminant of the form is defined for any degree, which yields a first invariant. If the degree of the form is greater than 3, then it can be shown that there are invariants algebraically independent of the discriminant. All these invariants can be viewed themselves as homogeneous polynomials, where the coefficients of the form are the variables of the invariant, which is clear in the case of the discriminant of a binary quadratic.

In the case of binary quintics, Clebsch [Cle1872] showed that the algebra generated by all invariants is generated by 4 elements, which he named A, B, C and R. His proof consisted mainly of explicit computations. Gordan gave a constructive way to find a finite set of generators for any given degree [GY1903, Chapter VI], while it was Hilbert who in 1888 proved the existence of such a set for the general case. As Hilbert's proof was not constructive, which was quite unusual in these times, it was received with mixed reactions. This grew into a small myth, which claims that Gordan reacted to the proof of Hilbert by saying "This is not Mathematics, it is Theology!" [Mcl2008].

Reconstruction

The reconstruction of forms is a more recent topic of research. The main application of these reconstructions is to find a model of a curve over a given field, given the values of invariants contained in this field. An important result in this topic is that of Mestre [Mes1991], who *(re)constructed* binary sextics from invariants. Given values for the (Igusa) invariants A, B, C, D and R of binary sextics, Mestre used quadratic covariants (a generalisation of invariants) to compute a binary sextic that attains these values up to some scaling factor. In the case of Mestre, these were hyperelliptic curves of genus 2. The method of Mestre was based on the work of Clebsch, who essentially used the same methods, although for a different purpose, namely finding explicit linear transformation between distinct forms.

A more general reconstruction method based on the work of Mestre was provided by Lercier and Ritzenthaler [LR2012]. This method allows the reconstruction of binary forms of arbitrary even degree. In this thesis, a similar result for binary forms of odd degree will be given. For the case of binary quintics, we will use this general result to provide an explicit way to reconstruct these forms over arbitrary base fields.

The main result is an explicit bijection between the set of binary forms up to linear transformations and the set of possible values of invariants of a binary quintic. This bijection is given in the following theorem:

Theorem 3.10. *Let k be an algebraically closed field of characteristic 0 or $p > 5$. Let $B_5 \subset S^5(V)$ denote the space of binary quintic forms over k which do not posses a threefold linear factor. Let A, B and C be as in Table 1. Then there is a bijection*

$$\begin{aligned} \mathrm{GL}_2(k)\backslash B_5 &\to \mathbb{P}^{(1,2,3)}(k), \\ [f] &\mapsto (A(f), B(f), C(f)). \end{aligned}$$

Moreover, the inverse is explicit in the sense that it maps $(a : b : c) \in \mathbb{P}^{(1,2,3)}(k)$ to $\tilde{f}$ as described by Lemma 3.5 or Lemma 3.6. This inverse maps points defined over any subfield $l \subset k$ to quintics $\tilde{f}$ with coefficients in l.

The inverse of the above map is established by giving a map $\mathbb{P}^{(1,2,3)}(k) \to B_5$, which is made explicit in Definition 3.8.

Analogues of this theorem for fields of characteristic 2, 3 or 5 are given in respectively Theorem 4.5, Theorem 4.7 and Theorem 4.8.

Thesis contents

We start by treating the work of Clebsch and Hilbert [Hil1993] to give a description of (classical) invariant theory. We will give an explicit set of

generators for the algebra of invariants of binary quintics over the field of complex numbers in Table 2.

The second chapter will focus on generalising the results from the first chapter to fields of arbitrary characteristic, as in the classical theory only the field of complex numbers was considered. We will present a theoretical method to find a set of invariants that fully describes all possible invariant values in Proposition 2.12. Finally in Theorem 2.18 we will define a map relating binary forms to their invariants, which will be our starting point for reconstructing binary quintics.

The reconstruction of binary quintics is performed in Chapter 3, where we will present a general method for reconstruction in Theorem 3.1. After considering some special cases, this will be used for proving the main theorem of this thesis for reconstruction of forms over fields of characteristic 0 and $p > 5$.

Finally, we will give a partial description of the ring of invariants of binary quintics for fields of small characteristic and a complete method for reconstructing binary quintics over these fields.

1 Classical invariant theory

In this chapter the basics of invariant theory are explained, based on the theory developed in the 19th century. This theory was first developed by Cayley and focuses on linear transformations of *complex forms*, homogeneous polynomials in two or more variables defined over $\mathbb{C}$. We will focus on the theory related to binary forms, homogeneous polynomials with 2 variables. Moreover, we will consider forms over arbitrary fields of characteristic 0 or $p > 0$, where most of the theory still remains valid. In some cases, we will restrict to the case of characteristic 0. For fields of different characteristic some results are no longer valid, which we will discuss more extensively in the next chapter.

The main reference for this chapter is the work of Clebsch [Cle1872] and the lecture notes of a course by Hilbert which took place in 1897 in Göttingen [Hil1993], which also both focus on the theory of complex forms.

Throughout this chapter, k will be a field of characteristic p, where p is either 0 or some prime number, $\overline{k}$ will be an algebraic closure of k and V a two-dimensional vector space over k with basis (x, z).

1.1 Definitions

We will start with defining *binary forms*, which are the objects we will study throughout this thesis.

Definition 1.1 (binary forms)**.** *Let $n \geq 1$ be an integer. Let $S^n(V)$ denote the n-th symmetric power of V. Then $S^n(V)$ is called the space of* binary forms *of degree n.*

The elements of $S^n(V)$ can be viewed as homogeneous polynomials of degree n with variables x and z, so that we can view a binary form f as a homogeneous polynomial $f \in k[x, z]$. We will now define an action of $\mathrm{GL}_2(k)$ on the space of binary forms, which corresponds to the linear transformations in the older literature.

Definition 1.2 (transformed form)**.** *Let $M \in \mathrm{GL}_2(k)$ be a matrix and $f \in S^n(V)$ be a binary form. Then we define $M \cdot f$ by setting*

$$(M \cdot f)(x, z) := f(M^{-1}(x, z)),$$

where M^{-1} acts on the column vector (x, z) by the standard action on vectors.

Remark 1.3. *Note that this action of $\mathrm{GL}_2(k)$ on $S^n(V)$ differs from the natural left action of $\mathrm{GL}_2(k)$ on $S^n(V)$ with basis (x, z).*

More explicitly, given a matrix $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and a binary form $f \in S^n(V)$, the transformed form $M \cdot f$ corresponds to a change of coordinates. For $x' = ax + bz$ and $z' = cx + dz$ we have $(M \cdot f)(x', z') = f(x, z)$.

These transformations of forms are related to isomorphisms between curves: if we have a form f of even degree without double roots and the characteristic of k is not equal to 2, then we can consider the hyperelliptic curve given by $y^2 = f(x, z)$. The curve given by $y^2 = (M \cdot f)(x, z)$ is then isomorphic to this curve, where the isomorphism is given by the described change of coordinates and where $y' = y$.

Conversely, for an algebraically closed field k of characteristic different from 2, all isomorphisms of hyperelliptic curves are given by such a linear transformation (see the article of Lercier and Ritzenthaler [LR2012, Section 1.2]). Hence there is a bijection between the set of orbits of binary forms (under this action) and the set of isomorphism classes of hyperelliptic curves.

We will describe these orbits in terms of functions on the space of binary forms which are in some sense invariant under the action of $\mathrm{GL}_2(k)$. We can then use these functions to characterise the orbits in term of their values when evaluating a representative in these functions.

Definition 1.4 (covariant and invariant)**.** *Let k be an infinite field. Let $n \geq 1$ and $m \geq 0$ be integers and let $G \subset \mathrm{GL}_2(k)$ be a subset. Let $C : S^n(V) \to S^m(V)$ be a polynomial map in the coefficients of $f \in S^n(V)$ and (x, z). If there exists $w \in \mathbb{Z}$ such that for all $M \in G$ and all $f \in S^n(V)$ the function C satisfies*

$$C(M \cdot f) = \det(M)^{-w} \cdot (M \cdot C(f)),$$

then C is called a covariant *of binary forms of degree n, of order m and weight w with respect to G. If it is of order $m = 0$, then we say that C is an* invariant *with respect to G.*

If $G = \mathrm{GL}_2(k)$, we call C a covariant (or invariant) (without explicitly specifying G).

In older literature, a general form $f = a_0x^n + a_1x^nz + ... + a_nz^n$ with abstract coefficients $a_0, ..., a_n$ is considered. Then for a covariant C the image $C(f)$, which is a binary form whose coefficients are polynomials in $a_0, ..., a_n$, is called a *covariant of f*. Thus a covariant can also be viewed as a polynomial $C(f) \in k[a_0, a_1, ..., a_n; x, z]$, which is uniquely defined as k is infinite.

Conversely, a polynomial $C \in k[a_0, a_1, ..., a_n; x, z]$ that is homogeneous with respect to (x, z) for an infinite field k defines a map $S^n(V) \to S^m(V)$ by evaluating it in the coefficients of $f \in S^n(V)$.

For a finite field k, we can use this polynomial C to define covariants. We say $C(f) \in k[a_0, a_1, ..., a_n; x, z]$ is a *covariant for k* if C is a covariant for $\overline{k}$ with respect to $\mathrm{GL}_2(\overline{k})$.

We will now look at a few examples of covariants.

Example 1.5. *Let $n \geq 1$ be an integer. The following maps are examples of covariants.*

1. *For any $m \geq 0$ the zero map $0 : S^n(V) \to S^m(V), f \mapsto 0$ is a covariant of order m (and weight w for all $w \in \mathbb{Z}$).*

2. *The identity map $\mathrm{id} : S^n(V) \to S^n(V), f \mapsto f$ is a covariant of order n and weight 0.*

3. *The map that maps $f \in S^n(V)$ to its discriminant is an invariant of weight $n(n-1)$.*

4. *The Hessian, which maps $f \in S^n(V)$ to the determinant*

$$\begin{vmatrix} \frac{\partial^2 f}{\partial x^2} & \frac{\partial^2 f}{\partial x \partial z} \\ \frac{\partial^2 f}{\partial x \partial z} & \frac{\partial^2 f}{\partial z^2} \end{vmatrix},$$

is a covariant of order $2(n-2)$ and weight 2.

Remark 1.6. *More generally, it is possible to allow the domain of a covariant to be $\bigoplus_{i=1}^{l} S^{n_i}(V)$ and let C be a polynomial in the coefficients of $(f_1, ..., f_l)$ and (x, z). In older literature such a polynomial is called a* simultaneous covariant of $f_1, f_2, ..., f_l$. *In this thesis, only the covariants of a single form are studied.*

We will now show that all the coefficients of a non-zero covariant $C \in k[a_0, ..., a_n][x, z]$ are homogeneous of some degree d in the coefficients of f. We will apply some well chosen transformations to a covariant $C : S^n(V) \to S^m(V)$ to deduce a relation between the degree of the form n, the order m, the weight w and this degree d.

For this, we first need a lemma we can use to relate equality of polynomials to equality of polynomial maps.

Lemma 1.7. *Let $n \geq 0$ be an integer, k be an infinite field and let $p \in k[X_1, ..., X_n]$. If for all $a \in k^n$ we have that $p(a) = 0$, then $p = 0$.*

Proof. We give a proof by induction. For $n = 0$ the result clearly holds.

Let $N \geq 1$ and suppose the result holds for all $n < N$. Let $p \in k[X_1, ..., X_{n-1}][X_n]$, then for all $a \in k^{n-1}$ we have that $p_a = p(a)(X_n) \in k[X_n]$ satisfies $p_a(b) = 0$ for all $b \in k$. As k is infinite, this implies $p_a = 0$ for all a. If we let $C_i \in k[X_1, ..., X_{n-1}]$ such that $p_a = C_0(a) + C_1(a)X_n + ... + C_t(a)X_n^t$ for all $a \in k^{n-1}$, it follows that $C_i(a) = 0$ for all $a \in k^{n-1}$ and $i \in \{1, ..., t\}$.

The induction hypothesis then implies $C_i = 0$ for all $i \in \{1, ..., t\}$, thus it follows that $p = 0$. □

An immediate consequence of this lemma is the following corollary.

Corollary 1.8. *Let $n \geq 0$ be an integer, k be an infinite field and let $p, q \in k[X_1, ..., X_n]$. If for all $a \in k^n$ we have that $p(a) = q(a)$, then $p = q$.* □

Proposition 1.9 (degree of a covariant)**.** *Let k be an infinite field. Let $n \geq 1, m \geq 0$ be integers and let $C : S^n(V) \to S^m(V)$ be a non-zero covariant of weight w. Then all coefficients of C are homogeneous of some degree $d \geq 0$ in the coefficients of f, which we will call the* degree *of C. Moreover, this degree satisfies $nd - 2w = m$.*

Proof. First, we assume I to be an invariant (or equivalently $m = 0$). For a general form $f = a_0x^n + a_1x^{n-1}z + ... + a_nz^n$, we can write $I(f) = \sum_t i_t \cdot a_0^{t_0}a_1^{t_1} \cdots a_n^{t_n}$ with $t = (t_0, t_1, ..., t_n) \in (\mathbb{Z}_{\geq 0})^{n+1}$, $i_t \in k$ (where $i_t = 0$ for almost all t) and $d_t := \sum_i t_i$. Consider the matrix $M = \begin{pmatrix} \lambda^{-1} & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$ for $\lambda \in k^*$. Then we find that

$$\begin{aligned} I(M \cdot f) &= \sum_t i_t \cdot (\lambda^n a_0)^{t_0} \cdot (\lambda^n a_1^{t_1}) \cdots (\lambda^n a_n)^{t_n} \\ &= \sum_t \lambda^{nd_t} \cdot i_t \cdot a_0^{t_0}a_1^{t_1} \cdots a_n^{t_n}, \end{aligned}$$

while on the other hand we have

$$(\det M)^{-w} I(f) = \lambda^{2w} \cdot \sum_t i_t \cdot a_0^{t_0}a_1^{t_1} \cdots a_n^{t_n}.$$

As k is infinite, equality can only hold for all $\lambda \in k^*$ and $f \in S^n(V)$ if we have $2w = nd_t$ for all t with $i_t \neq 0$. As this equality holds for all t with $i_t \neq 0$, it follows that indeed all the terms are homogeneous of the same degree $d = \frac{2w}{n}$.

Now suppose C is a covariant of order $m \geq 0$ and write $C(f) = \sum_{j=0}^m C_j(a_0, ..., a_n)x^j z^{m-j}$. Then we have

$$\begin{aligned} \det(M)^{-w} \cdot (M \cdot C(f)) &= \sum_{j=0}^m \lambda^{2w} \cdot C_j(a_0, ..., a_n)(\lambda x)^j (\lambda z)^{m-j} \\ &= \lambda^{2w+m} \cdot \sum_{j=0}^m C_j(a_0, ..., a_n)x^j z^{m-j} \end{aligned}$$

and

$$C(M \cdot f) = \sum_{j=0}^m C_j(\lambda^n a_0, ..., \lambda^n a_n)x^j z^{m-j}.$$

By Corollary 1.8, the above two polynomial maps are equal if and only all coefficients are equal as k is infinite. Therefore we have $\lambda^{2w+m}C_j(a_0,...,a_n) = C_j(\lambda^n a_0,...,\lambda^n a_n)$ for all $j \in \{0,...,m\}$. For fixed j, we can write C_j as a sum of monomials $i_t \cdot a_0^{t_0}a_1^{t_1}\cdots a_n^{t_n}$ similar to the invariant case.

Then we obtain that $2w + m = nt_1 + nt_2 + ... + nt_n = nd_t$ for all $t \in (\mathbb{Z}_{\geq 0})^{n+1}$ such that $i_t \neq 0$, as the equality holds for all $\lambda \in k^*$. Applying this to each of the coefficients C_j of C, we find that all coefficients are homogeneous of some degree d such that $nd - 2w = m$. □

Remark 1.10. *If we replace one λ by $\mu \in k^*$ in the matrix of the proof, then we find for all terms of C_j of a covariant C the two equalities $w + j = nt_0 + (n-1)t_1 + ... + t_{n-1}$ and $w + m - j = t_1 + 2t_2 + ... + nt_n$.*

So for fixed j both the expressions $i_0 = nt_0 + (n-1)t_1 + ... + t_{n-1}$, which is sometimes referred to as the weight of a monomial, and the expression $i_1 = t_1 + 2t_2 + ... + nt_n$ are constant for all terms of the polynomial C_j. A homogeneous polynomial in $a_0,...,a_n$ which satisfies this property is called isobaric of weight i_0.

This proposition tells us a lot about the coefficients of covariants: they are homogeneous in terms of the coefficients of the binary form, so it is easy to find the weight of a given covariant. For example, for a binary quadratic $f = a_0x^2 + a_1xz + a_2z^2$, its discriminant $a_1^2 - 4a_0a_2$ is an invariant which is homogeneous of degree 2 in the coefficients of f, hence of weight 2. Moreover, the proposition implies that only for specific combinations there can exist a covariant of given order and weight. In particular, we find that for forms of even degree n, all the non-zero covariants are of even order.

To conclude this section, we will consider linear combinations and compositions of covariants. If we look at the definition of a covariant, it is straightforward to check that linear combinations of covariants with the same weight and order are again covariants. Also, the composition of two covariants is again a covariant. This follows from the fact that linear combinations and compositions of polynomial maps are again polynomial maps and covariants are homogeneous by Proposition 1.9. This is summarized in the following proposition.

Proposition 1.11. *Let $n \geq 1$ and $m \geq 0$ be two integers.*

1. (addition and scalar multiplication) *Let $w \geq 0$ be an integer. Then the set of covariants $C : S^n(V) \to S^m(V)$ of degree d and order m is a k-vector space.*

2. (composition) *Let $l \geq 1$ be an integer. Let $C : S^n(V) \to S^l(V)$ and $C' : S^l(V) \to S^m(V)$ be two covariants of respective degrees d and d'. Then the composition $C' \circ C$ is a covariant of degree dd'.* □

1.2 Algebra of covariants

In this section we will study the algebra generated by the covariants of binary forms for a fixed degree n. If we view the covariants as polynomials, their product is simply their product as polynomials. The resulting ring is doubly graded with respect to the order m (i.e. the degree with respect to the basis (x, z) of V) and the degree d (i.e. the degree in the coefficients $a_0, ..., a_n$ of $f \in S^n(V)$). This ring is a subring of the ring $k[a_0, ..., a_n; x, z]$, which is summarized in the following proposition. We let $C_n^{m,d}(k)$ denote the vector space of covariants of degree d and order m and let $I_n^d(k) := C_n^{0,d}(k)$ denote the vector space of invariants of degree d.

Proposition 1.12 (Algebras of covariants and invariants)**.** *Let k be a field and let $n \geq 1$ be an integer. For $m \geq 0$ and $d \geq 0$, let $C_n^{m,d}(k)$ be the space of covariants of order m and degree d of degree n binary forms. Then the subring $\mathcal{C}_n(k)$ of the ring $k[a_0, ..., a_n; x, z]$ generated by the covariants $C : S^n(V) \to S^m(V)$ for all $m \geq 0$ is a bigraded ring, graded by the order m and degree d, and we have $\mathcal{C}_n(k) = \bigoplus_{(m,d)\in\mathbb{Z}^2_{\geq 0}} C_n^{m,d}(k)$.*
In particular, the subring $\mathcal{I}_n(k)$ generated by the invariants $I : S^n(V) \to S^0(V) \cong k$ is a graded ring, graded by the degree d, and we have $\mathcal{I}_n(k) = \bigoplus_{d\in\mathbb{Z}_{\geq 0}} I_n^d(k)$.

Proof. Consider the ring $R = k[a_0, .., a_n, x, z]$. For $f \in R$, write d for the degree of f with respect to $a_0, ..., a_n$ and m for the degree of f with respect to x, z. Then R is bigraded with respect to m and d. For any pair $(m, d) \in Z^2_{\geq 0}$ the vector space $C_n^{m,d}(k)$ is a subspace of R that is linearly independent from the others. Moreover, the subring generated by the covariants is closed under multiplication as the product of covariants is again a covariant. Thus it follows that the subring generated by the covariants is again graded. □

We will call $\mathcal{C}_n(k)$ the *algebra of covariants* and $\mathcal{I}_n(k)$ the *algebra of invariants*. For fields of characteristic 0, the elements in the algebra of covariants that are homogeneous with respect to the order m are exactly the covariants of order m with respect to the group $G = \mathrm{SL}_2(k)$, which we will show in the next proposition.

Remark 1.13. *The proof below also applies to fields of sufficiently large characteristic, i.e. larger than both the order m and degree n of the form. We will not need this, as we will only use this result to prove that the algebra of invariants is finitely generated in the case where the characteristic of k is 0.*

Proposition 1.14. *Let k be a field of characteristic 0. Let $n \geq 1$ be an integer and consider the algebra of covariants $\mathcal{C}_n(k)$. Then for any $m \geq 0$, the homogeneous elements of degree m with respect to (x, z) are covariants*

of order m with respect to $\mathrm{SL}_2(k)$. Moreover, if $C : S^n(V) \to S^m(V)$ is a covariant with respect to $\mathrm{SL}_2(k)$ that is homogeneous of degree d with respect to $a_0, ..., a_n$, then C is a covariant (of order m) with respect to $\mathrm{GL}_2(k)$.

Proof. Let $C \in \mathcal{C}_n(k)$ be homogeneous with respect to the order m. Then C can be written as sum $C = \sum_{d \in \mathbb{Z}_{\geq 0}} C_d$ of polynomials C_d that are homogeneous of degree d (in $a_0, ..., a_n$). These polynomials are covariants as the ring of covariants is graded by the degree (Proposition 1.12). Therefore they satisfy $C_d(M \cdot f) = M \cdot C_d(f)$ for all $M \in \mathrm{SL}_2(k)$. Thus it follows that C satisfies this property too.

Conversely let $C : S^n(V) \to S^m(V)$ be a covariant with respect to $G = \mathrm{SL}_2(k)$ that is homogeneous of degree d with respect to $a_0, ..., a_n$. Then we can follow the same reasoning as in Remark 1.10, where we consider the matrix with diagonal entries λ and λ^{-1}. In this case the determinant of the matrix is 1, so that if we write $C(f) = \sum_{j=0}^{m} C_j(a_0, ..., a_n) x^{m-j} z^j$ where each C_j is homogeneous of degree d, covariance implies $C_j(a_0, ..., a_n) = \lambda^{2j-m} C_j(\lambda^{-n} a_0, \lambda^{2-n} a_1, ..., \lambda^n a_n)$. This equality then implies that all C_j's are isobaric of respective weights $w + j$ where $2w = nd - m$, i.e. for every monomial $a_0^{t_0} a_1^{t_1} \cdots a_n^{t_n}$ in C_j with non-zero coefficient we have $nt_0 + (n-1)t_1 + ... + t_{n-1} = w + j$.

If we then look at the matrix $M = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & 1 \end{smallmatrix}\right)$ with $\lambda \in k^*$, we find that $(\det M)^{-w} \cdot M \cdot C(f) = \cdot \sum_{j=0}^{m} \lambda^{-w-j} C_j(f) x^{m-j} z^j$ while on the other hand we have $C_j(M \cdot f) = C_j(\lambda^{-n} a_0, ..., \lambda^{-1} a_{n-1}, a_n) = \lambda^{-w-j} \cdot C_j(f)$ as C_j is isobaric of weight $w + j$. This shows that C is covariant with respect to transformations of this shape. As $\mathrm{SL}_2(k)$ and the matrices M of this shape together generate $\mathrm{GL}_2(k)$, it follows that C is a covariant with respect to $\mathrm{GL}_2(k)$. □

Apart from linear combinations, multiplication and composition there is another method to construct more covariants out of other covariants. The last example of Example 1.5 is a special case of a more general construction described by Clebsch to obtain covariants.

This construction yields, given two covariants f and g and a positive integer h, a covariant that Clebsch called the *'Ueberschiebung'*. In English literature, this resulting covariant is called the *transvectant* and is defined as follows.

Definition 1.15 (transvectant)**.** *Let k be a field of characteristic 0. Let f, g be two binary forms over k with variables respectively (x, z) and (x', z') of respective degrees m_f and m_g and let $h > 0$ be a positive integer. Then we define the h-th* transvectant *of f and g to be the form*

$$(f, g)_h = \frac{(m_f - h)! \cdot (m_g - h)!}{m_f! \cdot m_g!} \left(\left(\frac{\partial}{\partial x} \frac{\partial}{\partial z'} - \frac{\partial}{\partial x'} \frac{\partial}{\partial z} \right)^h (f \cdot g) \right)_{(x', z') = (x, z)},$$

where the h-th power denotes the h-th composition of the operator.

We denote the first transvectant of f and g, i.e. when $h = 1$, by $(f, g) := (f, g)_1$.

Now suppose we have a binary form $f \in S^n(V)$ and two covariants C, C' of respective orders m and m' and degrees d and d'. Then the map $f \mapsto (C(f), C'(f))_h$ is a covariant of order $m + m' - 2h$ and degree $d + d'$. As for any $n \geq 0$ the identity map on $S^n(V)$ is a covariant, this implies that the transvectant of f with a covariant $C(f)$ of f is again a covariant of f. Thus the transvectant can be used to construct new covariants.

The main result of classical invariant theory is that given a field k of characteristic 0 and an integer $n \geq 0$, there exists a finite set of generators for the algebra of covariants $\mathcal{C}_n(k)$. The proof of this result is due to Hilbert, who was the first to show that the algebra of covariants is finitely generated when the base field is $\mathbb{C}$. Later a proof was provided by Gordan, which is treated extensively in the book of Grace and Young [GY1903, Chapter VI]. The proof of Gordan is constructive, so that it gives an explicit method to find a set of generators by taking transvectants, although it is quite impractical for larger n.

We will only need the following theorem, which asserts that the algebra of invariants is finitely generated.

Theorem 1.16 (Hilbert's finiteness theorem)**.** *Let k be a field of characteristic 0 and let $n \geq 1$ be an integer. Then the algebra $\mathcal{I}_n(k)$ of invariants of binary forms of degree n is finitely generated.*

Proof. See [Hil1993, p. 132] for a proof when $k = \mathbb{C}$. The proof in these notes can be generalised to arbitrary fields of characteristic 0. A more concise proof for these fields can be found in e.g. the book of Derksen and Kemper [DK2002, Theorem 2.2.10]. □

In the notes of Hilbert's lectures [Hil1993, Section I.7] it is shown that the dimensions of the vector spaces of invariants of fixed degree n and weight w can be computed using a power series expansion of a rational function.

Given a binary form $f = a_0x^n + a_1x^{n-1}z + ... + a_nz^n$ and an invariant $I = \sum c_t a_0^{t_0} a_1^{t_1} \cdots a_n^{t_n} \in k[a_0, ..., a_n; x, z]$ of degree d and weight w, the fact that I is an invariant implies that all terms satisfy $\sum_{i=0}^n t_i = d$ and $\sum_{i=0}^n it_i = w$.

Then Hilbert defines $\omega_n(d, w)$ to be the number of solutions to the equations $\sum_{i=0}^n t_i = d$ and $\sum_{i=0}^n it_i = w$ with $(t_0, t_1, ..., t_n) \in \mathbb{Z}_{\geq 0}^{n+1}$; these solutions correspond to all distinct monomials of degree d and weight w. Using the defining property of the invariants, Hilbert deduces relations between their monomials in order to determine the number of linearly independent invariants for a fixed degree d. This leads to the following result; for more details, we refer to the notes of the lectures by Hilbert [Hil1993, Section I.7].

Proposition 1.17. *Let $n \geq 1$, $d \geq 1$ and $w \geq 0$ be integers such that $nd = 2w$. Then the dimension of the vector space of invariants of forms of degree n which are of degree d and weight w is the coefficient of x^w in the power series expansion of*

$$\frac{\prod_{j=n+1}^{n+d}(1-x^j)}{\prod_{i=2}^{d}(1-x^i)}.$$

Proof. See [Hil1993, Equation (II), p. 54]. □

We can compute the weight by using the relation $2w = nd$ as seen in Proposition 1.9, so that one can explicitly determine the dimension of the space of invariants of a given degree d. For small values of n, this number is used to determine the number of generators needed and their respective orders in the notes of Hilbert's lectures [Hil1993].

For example, for quadratic forms ($n = 2$) the number of linearly independent invariants of degree d is the d-th coefficient of the power series expansion of $\frac{(1-x^{d+1})(1-x^{d+2})}{1-x^2}$, which is equal to 0 when d is odd and 1 when d is even. So it follows that for the algebra of invariants is generated by a single invariant of degree 2, which is the discriminant of the form.

When n increases, these calculations become increasingly difficult. For the cases $n \in \{3, 4, 5\}$ they can be found in the notes of Hilbert's lectures [Hil1993, Section I.7]. Using Proposition 1.17, it is shown that the algebra $\mathcal{I}_5$ is generated by four invariants of respective degrees 4, 8, 12 and 18. In the next section we will explicitly determine a set of four generators of the algebra of invariants for a binary quintic.

1.3 Invariants of a binary quintic

To illustrate the results of the previous section, we will now determine the invariants generating the algebra $\mathcal{I}_5$ of a binary quintic for fields of characteristic 0. We can follow the computations from the classical invariant theory over $\mathbb{C}$ studied in the 19th century. By a result of Geyer [Gey1974] it follows that this can be generalized to fields of characteristic $p > 5$, which we will discuss later, in Chapter 2.

1.3.1 Clebsch invariants

As seen before, the algebra $\mathcal{I}_5$ is generated by 4 invariants of respective degrees 4, 8, 12 and 18. Between those, there exists a polynomial relation of degree 36 (in the coefficients of f). Such a polynomial relation between generators of an algebra is called a *syzygy* in older literature. We will follow the approach of Clebsch [Cle1872, § 73] to determine all invariants (and some covariants). In order to follow these computations, we will for now assume that the field k is of characteristic 0.

The first covariant is the identity map $S^5(V) \to S^5(V)$, which we will denote by f. Then we start by defining a quadratic covariant i, which is a transvectant of f with itself: $i = (f, f)_4$. In terms of the coefficients, given a form $f = a_0x^5 + a_1x^4z + a_2x^3z_2 + a_3x^2z^3 + a_4xz^5 + a_5z^5 \in S^5(V)$, we have

$$\begin{aligned} i(f) = &(3/50a_2^2 - 4/25a_1a_3 + 2/5a_0a_4)x^2 \\ &+ (1/25a_2a_3 - 6/25a_1a_4 + 2a_0a_5)xz \\ &+ (3/50a_3^2 - 4/25a_2a_4 + 2/5a_1a_5)z^2. \end{aligned}$$

All invariants and covariants we will use throughout this thesis can then be computed as transvectants of other covariants. They are described in Table 1.

covariant	**definition**	**order**	**degree**	**weight**
f	f	5	1	0
i	$(f, f)_4$	2	2	4
j	$-(i, f)_2$	3	3	6
τ	$(j, j)_2$	2	6	14
θ	(i, τ)	2	8	19
α	$(i^2, f)_4$	1	5	12
β	(i, α)	1	7	17
γ	(τ, α)	1	11	27
δ	(θ, α)	1	13	32
A	$(i, i)_2$	0	4	10
B	$(i, \tau)_2$	0	8	20
C	$(\tau, \tau)_2$	0	12	30
R	$(\theta, \alpha^2)_2$	0	18	45
M	(β, α)	0	12	30
N	(γ, α)	0	16	40

Table 1: Clebsch covariants of a binary quintic

The invariants listed in this table are not algebraically independent: the invariants M and N are polynomials in the invariants A, B and C as we have $N = \frac{1}{2}(AC - B^2)$ and $M = 2AB - 3C$. In terms of these invariants, we have a syzygy given by

$$R^2 = -\frac{1}{2}(AN^2 - 2BMN + CM^2). \tag{1}$$

The invariants found above form a set of generators for the algebra of invariants, which is shown by the following proposition.

Proposition 1.18. *Let k be either $\mathbb{Q}$ or $\mathbb{C}$. Then the algebra $\mathcal{I}_5(k)$ is generated by A, B, C and R, as defined in Table 1. Moreover, the ideal of relations between these invariants is generated by Equation (1).*

Proof. For $k = \mathbb{C}$ this is exactly the theorem on the invariants of binary quintics in the notes of Hilbert's lectures, see [Hil1993, p. 59]. As A, B, C and R have rational coefficients, it follows that for $k = \mathbb{Q}$ this set generates an algebra $\mathbb{Q}[A, B, C, R] \subset \mathcal{I}_5(\mathbb{Q})$. It remains to show the reverse inclusion.

To prove this, we use the fact that the set of fixed points of the automorphism group of $\mathbb{C}$ is exactly $\mathbb{Q}$, i.e. $\mathbb{C}^{\mathrm{Aut}(\mathbb{C})} = \mathbb{Q}$. This can be seen by combining two results from the article of Yale [Yal1966], namely Theorem 2 and Theorem 7. The first says that any automorphism on $\mathbb{C}$ extends the identity map on $\mathbb{Q}$, the second claims any automorphism of a subfield of $\mathbb{C}$ can be extended to an automorphism of $\mathbb{C}$. Hence for any $\alpha \in \mathbb{C} \setminus \mathbb{Q}$, we can construct an automorphism that does not fix α. If α is algebraic, we can consider a normal closure of $\mathbb{Q}(\alpha)$ in $\mathbb{C}$ and take any automorphism in the Galois group that does not leave α fixed. If α is transcendental, we can consider the automorphism $\mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha), \alpha \mapsto \alpha^{-1}$. Thus it follows that only $\mathbb{Q}$ is fixed by all automorphisms on $\mathbb{Q}$.

Now let $F \in \mathcal{I}_5(\mathbb{Q})$, then we have $F \in \mathcal{I}_5(\mathbb{C}) = \mathbb{C}[A, B, C, R]$ and so we can write $F = \sum c_{a,b,c,r} A^a B^b C^c R^r$ with $c_{a,b,c,r} \in \mathbb{C}$, $a, b, c \in \mathbb{Z}_{\geq 0}$ and $r \in \{0, 1\}$. For $\sigma \in \mathrm{Aut}(\mathbb{C})$ we have $F = \sigma(F)$ as we have $F \in \mathcal{I}_5(\mathbb{Q})$, and we also have $\sigma(F) = \sum \sigma(c_{a,b,c,r})\sigma(A)^a \sigma(B)^b \sigma(C)^c \sigma(R)^r = \sum \sigma(c_{a,b,c,r}) A^a B^b C^c R^r$. But then $F - \sigma(F) = 0$ and the fact that equation (1) generates the ideal of relations imply $\sigma(c_{a,b,c,r}) = c_{a,b,c,r}$ for all a, b, c, r. As this holds for any $\sigma \in \mathrm{Aut}(\mathbb{C})$, we find $c_{a,b,c,r} \in \mathbb{Q}$ for all a, b, c, r, hence $F \in \mathbb{Q}[A, B, C, R]$, so that $\mathbb{Q}[A, B, C, R] = \mathcal{I}_5(\mathbb{Q})$. □

1.3.2 Arithmetic invariants

For a general form $f = a_0 x^5 + a_1 x^4 z + ... + a_5 z^5$, the polynomials corresponding to the covariants in Table 1 have rational coefficients. In order to have a well-defined and meaningful reduction modulo p for primes p, we can scale them in such a way that we obtain primitive polynomials in $\mathbb{Z}[a_0, a_1, ..., a_5, x, z]$ (i.e. the greatest common divisor of their coefficients equals 1).

In addition, we take linear combinations of the invariants of respective weights 4, 8 and 12 in such a way there are no non-trivial relations between the reduced invariants modulo p for every prime p. These linear combinations are given in the table below. We will refer to these covariants as *arithmetic covariants* and similarly we call the invariants among those *arithmetic invariants*, which is a term introduced by Igusa [Igu1960, Section 3] for the case of binary sextics.

The arithmetic invariants are defined in Table 2. In terms of these invariants, the discriminant Δ of the quintic is given by $\Delta = 4I_8 - 3I_4^2$; it is an invariant of degree 8.

covariant	definition	order	degree	weight
I_4	$2^{-1} \cdot 5^4 \cdot A$	0	4	10
I_8	$2^{-1} \cdot 5^5 \cdot 47 \cdot A^2 - 2^2 \cdot 5^5 \cdot B$	0	8	20
I_{12}	$2^{-1} \cdot 3 \cdot 5^{10} \cdot A^3 - 2^5 \cdot 3^{-1} \cdot 5^{10} \cdot C$	0	12	30
I_{18}	$2^8 \cdot 3^{-1} \cdot 5^{15} \cdot R$	0	18	45
α'	$2^2 \cdot 5^4 \cdot \alpha$	1	5	12
β'	$2^3 \cdot 5^6 \cdot \beta$	1	7	17
γ'	$2^5 \cdot 5^{10} \cdot \gamma$	1	11	27
δ'	$2^6 \cdot 5^{11} \cdot \delta$	1	13	32
f	f	5	1	0

Table 2: Arithmetic covariants of a binary quintic

1.3.3 Computation of invariants

The author's implementation of these invariants in SageMath is part of version 8.4 and later; see https://trac.sagemath.org/ticket/25395. An example of the functionality can be found below. This implementation is part of the thesis work.

Example 1.19 (Computation of invariants in SageMath)**.**

```
""" Most of the invariants and covariants described in this section
    are available as methods of the BinaryQuintic class in Sage, which
    can be constructed with the invariant_theory.binary_quintic function.
    For example, one can compute the covariant i as follows:"""

sage: R.<a0,a1,a2,a3,a4,a5> = QQ[]
sage: S.<x,y> = R[]
sage: p = a0*x^5 + a1*x^4*y + a2*x^3*y^2 + a3*x^2*y^3 + a4*x*y^4 + a5*y^5
sage: quintic = invariant_theory.binary_quintic(p)
sage: quintic.i_covariant()
(3/50*a2^2 - 4/25*a1*a3 + 2/5*a0*a4)*x^2 + (1/25*a2*a3 - 6/25*a1*a4
+ 2*a0*a5)*x*y + (3/50*a3^2 - 4/25*a2*a4 + 2/5*a1*a5)*y^2

""" The method clebsch_invariants can be used to compute
    the Clebsch invariants A, B, C and R of a binary quintic."""

sage: R.<x0, x1> = QQ[]
sage: p = 2*x1^5 + 4*x1^4*x0 + 5*x1^3*x0^2 + 7*x1^2*x0^3 - 11*x1*x0^4 \
      + x0^5
sage: quintic = invariant_theory.binary_quintic(p, x0, x1)
sage: quintic.clebsch_invariants()
{'A': -276032/625,
 'B': 4983526016/390625,
 'C': -247056495846408/244140625,
 'R': -1489789728286968473 76/30517578125}

""" Alternatively, one can use the arithmetic_invariants method."""

sage: R.<x0, x1> = QQ[]
sage: p = 2*x1^5 + 4*x1^4*x0 + 5*x1^3*x0^2 + 7*x1^2*x0^3 - 11*x1*x0^4 \
      + x0^5
sage: quintic = invariant_theory.binary_quintic(p, x0, x1)
```

```
sage: quintic.arithmetic_invariants()
{'I12': -1156502613073152,
 'I18': -12712872348048797642752,
 'I4': -138016,
 'I8': 14164936192}

""" It is also possible to compute the transvectant of two
    algebraic forms, using the transvectant function."""

sage: from sage.rings.invariants.invariant_theory import AlgebraicForm, \
          transvectant
sage: R.<a0,a1,a2,a3,a4,a5,x0,x1> = QQ[]
sage: p = a0*x1^5 + a1*x1^4*x0 + a2*x1^3*x0^2 + a3*x1^2*x0^3 + a4*x1*x0^4 \
      + a5*x0^5
sage: f = AlgebraicForm(2, 5, p, x0, x1)
sage: transvectant(f, f, 4)
Binary quadratic given by 3/50*a3^2*x0^2 - 4/25*a2*a4*x0^2
+ 2/5*a1*a5*x0^2 + 1/25*a2*a3*x0*x1 - 6/25*a1*a4*x0*x1 + 2*a0*a5*x0*x1
+ 3/50*a2^2*x1^2 - 4/25*a1*a3*x1^2 + 2/5*a0*a4*x1^2
```

2 Invariant theory for general fields

In the previous chapter we have seen classical invariant theory, which only considers the field of complex numbers. After further progress in algebraic geometry, more general applications of invariant theory were studied. In this chapter we will discuss this more general theory and use the results to determine the invariants of a binary quintic for arbitrary fields.

Our approach will be to follow the same strategy as Rovetta [Rov2017], which uses more recent results to find covariants in fields of small characteristic.

Throughout this chapter, k denotes an arbitrary field, S an integral domain and $n \geq 1$ a positive integer.

2.1 Invariants of $(\mathbb{P}^1)^n$

Instead of looking at invariants of binary forms, in this section we will focus on invariants of $(\mathbb{P}^1(k))^n$. The space $(\mathbb{P}^1(k))^n$ is closely related to the space $S^n(V)$ of binary forms of degree n, as we can consider the linear factors (over the algebraic closure) of a binary form.

The coefficients of these linear factors may be viewed as points in $\mathbb{P}^1(k)$, so that a binary form $f = \prod_{i=1}^{n}(\alpha_i x + \beta_i z) \in S^n(V)$ corresponds to $((\alpha_1 : \beta_1), ..., (\alpha_n : \beta_n)) \in (\mathbb{P}^1(k))^n$ up to permutation and suitable scaling of the coordinates. The main advantage of considering invariants of the corresponding polynomial ring $k[\alpha_1, \beta_1, ..., \alpha_n, \beta_n]$ is that its algebra of invariants will be essentially the same for all fields.

If we consider the space $(k^2 \setminus \{(0,0)\})^n$, we define the action of $\mathrm{GL}_2(k)$ on it as follows.

Definition 2.1. *Let $M \in \mathrm{GL}_2(k)$ be a matrix and $x = ((\alpha_1, \beta_1), ..., (\alpha_n, \beta_n)) \in (k^2 \setminus \{(0,0)\})^n$ a point. Then we define*

$$M \cdot x = ((\alpha_1', \beta_1'), ..., (\alpha_n', \beta_n')),$$

where $\begin{pmatrix} \alpha_i' & \beta_i' \end{pmatrix} = \begin{pmatrix} \alpha_i & \beta_i \end{pmatrix} M^{-1}$ for $i = 1, ..., n$.

Note that this action induces an action on $(\mathbb{P}^1(k))^n$.

We then look at the ring of polynomials $k[\alpha_1, \beta_1, ..., \alpha_n, \beta_n]$, on which we have an induced right action of $\mathrm{GL}_2(k)$ by setting $P \cdot M(\alpha_1, \beta_1, ..., \alpha_n, \beta_n) = P(\alpha_1', \beta_1', ..., \alpha_n', \beta_n')$. This leads us to the following definition:

Definition 2.2 (invariant)**.** *Let k be an algebraically closed field and $w \in \mathbb{Z}$. We say that a polynomial $P \in k[\alpha_1, \beta_1, ..., \alpha_n, \beta_n]$ is an* invariant of weight *w with respect to $G \subset \mathrm{GL}_2(k)$ if $P \cdot M = \det(M)^{-w} P$ for all $M \in G$.*

If $G = \mathrm{GL}_2(k)$, then we call P an invariant (without explicitly specifying G).

Example 2.3. *Let $n = 2$, then $P = \alpha_1\beta_2 - \alpha_2\beta_1$ is an invariant of weight 1. It corresponds to a root of the discriminant $b^2 - 4ac$ of the binary form $f = ax^2 + bxz + cz^2$.*

We will show for polynomials that being an invariant is equivalent to being a *regular bracket polynomial*, which is defined as follows:

Definition 2.4 (regular and bracket polynomials)**.** *Let S be a commutative ring. Let $P \in S[\alpha_1, \beta_1, ..., \alpha_n, \beta_n]$ be a polynomial, then we say that*

- *P is* regular of degree d *if for every monomial $\alpha_1^{s_1}\beta_1^{t_1} \cdots \alpha_n^{s_n}\beta_n^{t_n}$ that appears in P we have $s_i + t_i = d$ for all $i \in \{1, ..., n\}$;*
- *P is a* bracket *if $P = [i, j] := \alpha_i\beta_j - \alpha_j\beta_i$ for some distinct $i, j \in \{1, ..., n\}$;*
- *P is a* bracket polynomial *if it is an element of the subalgebra $\mathcal{B}(n) \subset S[\alpha_1, \beta_1, ..., \alpha_n, \beta_n]$ generated by the brackets.*

Lemma 2.5 (Geyer)**.** *Let k be an algebraically closed field. A polynomial $P \in k[\alpha_1, \beta_1, ..., \alpha_n, \beta_n]$ is an invariant if and only if it is a regular bracket polynomial.*

Proof. First we will show that a regular bracket polynomial is an invariant. Every bracket is an invariant with respect to $\mathrm{SL}_2(k)$, which can be seen as follows: if we write v_i for the row vector (α_i, β_i), then $[i, j] = v_i N v_j^T$ for $N = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Since $M^{-1}N(M^{-1})^T = N$ for all $M \in \mathrm{SL}_2(k)$, it follows that $[i, j] \cdot M = [i, j]$. This implies that every bracket polynomial is an invariant with respect to $\mathrm{SL}_2(k)$.

Moreover, every regular polynomial of degree d scales by a power λ^{-nd} if transformed by a matrix $M = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda \end{smallmatrix}\right)$ with $\lambda \in k^*$. Every bracket is of degree 2 with respect to $(\alpha_1, \beta_1, ..., \alpha_n, \beta_n)$, hence for a bracket polynomial any monomial is of even degree with respect to $(\alpha_1, \beta_1, ..., \alpha_n, \beta_n)$. A regular bracket polynomial is homogeneous of degree nd with respect to $(\alpha_1, \beta_1, ..., \alpha_n, \beta_n)$, hence for a regular bracket polynomial nd is necessarily even. Thus it follows that $\lambda^{nd} = (\det M)^{nd/2}$ is a power of the determinant for regular bracket polynomials. As k is algebraically closed, every matrix $B \in \mathrm{GL}_2(k)$ can be written as a product $B = MN$ of a diagonal matrix M as above such that $\lambda^2 = \det B$ and some matrix $N \in \mathrm{SL}_2(k)$. Thus a regular bracket polynomial is an invariant (with respect to $\mathrm{GL}_2(k)$).

The converse holds as well and a full proof of this fact was given by Geyer, see [Gey1974, Satz 5, p. 51]. □

We can generalize this result to integral domains, but in order to do so we first need to extend our definition of invariants.

Definition 2.6 (invariant)**.** *Let S be an integral domain and let k be its fraction field. Let $\overline{k}$ be an algebraic closure of k. We say that a polynomial $P \in S[\alpha_1, \beta_1, ..., \alpha_n, \beta_n]$ is an* invariant of weight w *with respect to $G \subset \mathrm{GL}_2(\overline{k})$ if there exists $w \in \mathbb{Z}$ such that for all $M \in G$ we have $P \cdot M = \det(M)^{-w} P$.*

If $G = \mathrm{GL}_2(\overline{k})$, we call P an invariant (without explicitly specifying G).

As seen, the points of $(\mathbb{P}^1)^n$ are related to binary forms of order n, where a binary form corresponds to an n-tuple which is determined up to permutation. So in order to find a correspondence between invariants of $(\mathbb{P}^1)^n$ and those of binary forms, we need to consider the regular bracket polynomials that are invariant under pairwise permutation of the coordinates.

Definition 2.7 (symmetric polynomial)**.** *Let k be a field. Let $n \geq 1$ be an integer and let S_n be the symmetric group acting on $\{1, ..., n\}$. Let $P \in k[\alpha_1, \beta_1, ..., \alpha_n, \beta_n]$ be a polynomial. We say that P is* symmetric *if for all $\sigma \in S_n$ we have*

$$P(\alpha_1, \beta_1, ..., \alpha_n, \beta_n) = P(\alpha_{\sigma(1)}, \beta_{\sigma(1)}, ..., \alpha_{\sigma(n)}, \beta_{\sigma(n)}).$$

Definition 2.8 (ring of symmetric regular bracket polynomials)**.** *Let k be a field and let $n \geq 1$ be an integer. We define the ring $I_n(k) \subset k[\alpha_1, \beta_1, ..., \alpha_n, \beta_n]$ to be the ring generated by all symmetric regular bracket polynomials, and call this the* ring of symmetric regular bracket polynomials.

Note that in the definition above the elements $P \in I_n(k)$ are not necessarily regular polynomials, but the homogeneous parts of P are regular.

To conclude this section, we will show there is an isomorphism between the ring $\mathcal{I}_n(k)$ of invariants of binary forms of degree n and the ring $I_n(k)$ of symmetric regular bracket polynomials, a result that is an immediate consequence of a theorem in the article of Rovetta [Rov2017].

Given a binary form $a_0 x^n + a_1 x^{n-1} z + ... + a_{n-1} x z^{n-1} + a_n z^n$ with abstract coefficients $a_0, ..., a_n$, we can formally write this form as product $f = \prod_{i=1}^{n} (\alpha_i x - \beta_i z)$. We can then express the coefficients a_i in terms of the α_i and β_i, e.g. $a_0 = \alpha_1 \cdots \alpha_n$. This defines a map $k[a_0, ..., a_n] \to k[\alpha_1, \beta_1, ..., \alpha_n, \beta_n]$. The corresponding map induces an isomorphism of the rings $\mathcal{I}_n(k)$ and $I_n(k)$.

Theorem 2.9 (Rovetta)**.** *Let k be a field. Let*

$$\begin{aligned} \Phi : k[a_0, a_1, ..., a_n] &\to k[\alpha_1, \beta_1, ..., \alpha_n, \beta_n] \\ a_j &\mapsto (-1)^j \alpha_1 \cdots \alpha_n \sigma_j\left(\frac{\beta_1}{\alpha_1}, \ldots, \frac{\beta_n}{\alpha_n}\right), \end{aligned}$$

where σ_j represents the j-th elementary symmetric polynomial in n variables. Then Φ induces an isomorphism of k-algebras between the ring $\mathcal{I}_n(k)$ of invariants of binary forms of degree n and the ring $I_n(k)$ of symmetric regular bracket polynomials.

Proof. See [Rov2017, Theorem 1]. □

2.2 Algebra of invariants

We will now look into invariants of binary quintics again. In the case of the complex numbers, we saw that the algebra of invariants was finitely generated, a result by Hilbert (see Theorem 1.16). This is a general fact, that holds for fields of arbitrary characteristic.

Theorem 2.10 (Hilbert's finiteness theorem for arbitrary fields)**.** *Let k be an algebraically closed field and let $n \geq 1$ be an integer. Then the algebra $\mathcal{I}_n(k)$ of invariants of binary forms of degree n is finitely generated.*

Proof. This result can be seen as a consequence of a more general result of Nagata [Nag1963, Main Theorem] (see also [DK2002, Theorem 2.2.16]), saying that for a *reductive* group G acting on a finitely generated k-algebra R, the ring of G-invariants is finitely generated. Note that in this case G-invariant means the point is fixed with respect to the action of G on R. For a definition of being reductive we refer to the book of Derksen and Kemper [DK2002, Section 2.2.2]. For our purpose it is enough to note that both SL_2 and S_n are reductive groups, see also [DK2002, Section 2.2.2], so that we can apply the result to the ring of regular polynomials in $\alpha_1, \beta_1, ..., \alpha_n, \beta_n$.

Let us consider the ring of regular polynomials that are invariant with respect to $\mathrm{SL}_2(k)$ as defined in Definition 2.2. The ring of regular polynomials is finitely generated, generated by the monomials $\prod_i \alpha^{t_i}\beta^{1-t_i}$ with $t = (t_1, ..., t_n) \in \{0, 1\}^n$. Also, the polynomials that are invariant with respect to $\mathrm{SL}_2(k)$ are fixed with respect to the action of $\mathrm{SL}_2(k)$ on this ring, hence by the result of Nagata ring of regular polynomials that are invariant with respect to $\mathrm{SL}_2(k)$ is finitely generated. Moreover, the ring of regular polynomials that are invariant with respect to $\mathrm{SL}_2(k)$ is exactly the ring of invariants with respect to $\mathrm{GL}_2(k)$. If we then consider the S_n-invariants of this ring and apply the result of Nagata again, it follows that the ring of invariants $\mathcal{I}_n(k)$ is finitely generated. □

In general, it is hard to compute an explicit set of generators. For the field of complex numbers we found a set of generators in Section 1.3. The arithmetic invariants found in Subsection 1.3.2 can be reduced modulo p for any prime p. For our goal of reconstructing binary forms, it will be sufficient to consider the algebra generated by these invariants. Results of Geyer [Gey1974] suggest they generate the algebra of invariants when $p > 5$, however we were unable to prove this general fact.

For fields of small positive characteristic p, the reduction modulo p of the set of arithmetic invariants is not necessarily a set of generators and we need to do separate computations for these cases. For the purpose of reconstructing binary forms, it turns out to be sufficient to compute not a set of generators (see Proposition 4.1) but a *separating subset*. For the definition of these subsets, we consider *linear algebraic groups*, which are

affine varieties G over an algebraically closed field k with a group operation such that group multiplication $m : G \times G \to G$ and inversion $i : G \to G$ are morphisms of affine varieties. We say G acts *regularly* on an affine variety X if the action $\mu : G \times X \to X$ is a morphism.

Definition 2.11 (separating subset)**.** *Let k be an algebraically closed field. Let X be an affine k-variety and let G be a linear algebraic group that acts regularly on X. A subset $S \subset k[X]^G$ is said to be* separating *if for any two points $x, y \in X(k)$ we have that if there exists $I \in k[X]^G$ such that $I(x) \neq I(y)$, then there exists $I' \in S$ such that $I'(x) \neq I'(y)$.*

It will be sufficient for our purposes to consider a separating subset instead of a set of generators. In the following proposition, we will show that knowing the value $I(f)$ for $I \in \mathcal{I}_n$ and $f \in S^n(V)$ is equivalent to knowing $J(f)$ for all $J \in S$ where S is a separating subset.

For this we will consider the ring $R = I_n(k)$ of regular bracket polynomials, with k algebraically closed, which is finitely generated (see also the proof of Theorem 2.10). Choose generators $P_1, ..., P_s$ so that we can write $R = k[P_1, ..., P_s]$. Then if we let $R = k[X_1, ..., X_s]/J$ for J some ideal, we can let $X = Z(J) \subset k^s$ so that we have $k[X] = R$. Moreover, $G = S_n$ acts regularly on X and we have $k[X]^G = R^G = \mathcal{I}_n(k)$ (see Theorem 2.9).

Proposition 2.12. *Let k be an algebraically closed field and let $\mathcal{I}_n(k)$ be its algebra of invariants of degree n binary forms. Let $R = k[P_1, ..., P_s] = k[X_1, ..., X_s]/J$ be the ring of regular bracket polynomials, let $X = Z(J) \subset k^s$ and let $G = S_n$. Let $A = \{I_1, ..., I_t\} \subset \mathcal{I}_n(k)$ be a finite separating subset.*

Then for all $f, g \in S^n(V)$ we have that if $I_i(f) = I_i(g)$ for all $i \in \{1, ..., t\}$, then $I(f) = I(g)$ for all $I \in \mathcal{I}_n(k)$.

Proof. Let φ be the map $\varphi : S^n(V) \to \mathrm{Hom}_{k\text{-alg}}(\mathcal{I}_n, k)$, where $\varphi(f)(I) = I(f)$ for all $f \in S^n(V)$ and $I \in \mathcal{I}_n$ and let ε be the map $\varepsilon : \mathrm{Hom}_{k\text{-alg}}(\mathcal{I}_n, k) \to k^t$, where $\varepsilon(\phi) = (\phi(I_1), \phi(I_2), ..., \phi(I_t))$ for all $\phi \in \mathrm{Hom}_{k\text{-alg}}(\mathcal{I}_n, k)$. Proving the claim is then equivalent to proving that ε is injective on the image of φ.

Now let ψ be the map $\psi : (k^2)^n \to \mathrm{Hom}_{k\text{-alg}}(R, k)$, where $\psi(x)(g) = g(x)$ for all $x \in (k^2)^n$ and $g \in R$, where we consider g as polynomial $g \in k[\alpha_1, \beta_1, ..., \alpha_n, \beta_n]$. Let r be the restriction map $r : \mathrm{Hom}_{k\text{-alg}}(R, k) \to \mathrm{Hom}_{k\text{-alg}}(\mathcal{I}_n, k)$ and let s be the (surjective) map $s : (k^2)^n \to S^n(V), ((\alpha_i, \beta_i))_i \mapsto \prod_{i=1}^n (\alpha_i x + \beta_i z)$. Then we have $\varphi \circ s = r \circ \psi$, so proving the claim is then equivalent to proving that ε is injective on the image of $r \circ \psi$.

Suppose that ε is not injective on the image of $r \circ \psi$, then there are $\overline{f}, \overline{g} \in (k^2)^n$ such that $(r \circ \psi)(\overline{f}) \neq (r \circ \psi)(\overline{g})$ and $\varepsilon((r \circ \psi)(\overline{f})) = \varepsilon((r \circ \psi)(\overline{g}))$. As we have $(r \circ \psi)(\overline{f}) \neq (r \circ \psi)(\overline{g})$, there is $I \in \mathcal{I}_n = k[X]^G$ such that $(r \circ \psi)(\overline{f})(I) \neq (r \circ \psi)(\overline{g})(I)$. Moreover, we have $(r \circ \psi)(\overline{f})(I) = r(\psi(\overline{f}))(I) = \psi(\overline{f})(I)$ and similarly $(r \circ \psi)(\overline{g})(I) = \psi(\overline{g})(I)$.

Then we note we can identify X with $\mathrm{Hom}_{k\text{-alg}}(R, k)$, where $x \in X$ corresponds with the evaluation map in x. Under this correspondence, we

have that $\psi(\overline{f}), \psi(\overline{g}) \in \mathrm{Hom}_{k\text{-alg}}(R, k)$ correspond with some $x, y \in X$ such that $I(x) = \psi(\overline{f})(I)$ and $I(y) = \psi(\overline{g})(I)$. But then the assumption that A is a separating subset combined with the notion that $I(x) \neq I(y)$ for some $I \in \mathcal{I}_n$ implies that there is some $i \in \{1, ..., t\}$ such that $\psi(\overline{g})(I_i) \neq \psi(\overline{g})(I_i)$, which contradicts our assumption that $\varepsilon((r \circ \psi)(\overline{f})) = \varepsilon((r \circ \psi)(\overline{g}))$. Hence it follows that ε is injective on the image of φ. □

In Chapter 4 we will look into separating subsets for the rings of invariants of binary quintics for fields of prime characteristic $p < 5$.

2.3 Weighted projective spaces

To conclude this chapter, we will study the relation between the orbits of forms under the action of $\mathrm{GL}_2(k)$ and their values when evaluated in the invariants. As seen in Theorem 2.10, the algebra of invariants is generated by a finite number of invariants.

However, if we take two distinct representatives of an orbit, the values of their invariants differ by a power of the determinant of the corresponding transformation matrix. Therefore we use the concept of a weighted projective space to 'scale' the values of the invariants in a proper way.

Definition 2.13 (weighted projective space)**.** *Let k be an algebraically closed field. Let $m \geq 0$ be an integer and let $d_0, ..., d_m$ be positive integers. Then the set $(k^{m+1} \setminus \{\mathbf{0}\})/\sim$, where $\sim$ is the equivalence relation given by*

$$(x_0, ..., x_m) \sim (y_0, ..., y_m) \Leftrightarrow \exists \lambda \in k^* : x_i = \lambda^{d_i} y_i \text{ for } i \in \{0, ..., m\},$$

is called the weighted projective space *of dimension m and weights $(d_0, ..., d_m)$, which is denoted by $\mathbb{P}^{(d_0,...,d_m)}(k)$.*

As we want to reconstruct binary quintics over arbitrary fields, we want to consider points in this space defined over a base field k, which are defined as follows.

Definition 2.14 (k-rational points)**.** *Let k be a field and let $\overline{k}$ be an algebraic closure of k. Let $\mathbb{P}^{(d_0,...,d_m)}(\overline{k})$ be the weighted projective space of dimension m and weights $(d_0, ..., d_m)$. Given a point $P \in \mathbb{P}^{(d_0,...,d_m)}(\overline{k})$, we say P is a* k-rational point *(or equivalently P* is defined over *k) if there are $x_0, ..., x_m \in k$ such that $P = (x_0 : ... : x_m)$.*

There is an equivalent definition for points being defined over k, which is very similar to the definition of points defined over k for regular projective spaces.

Proposition 2.15. *Let k be a field, let $\overline{k}$ be an algebraic closure of k and let k^{sep} be the separable closure of k in $\overline{k}$. Let $\mathbb{P}^{(d_0,...,d_m)}(\overline{k})$ be the weighted projective space of dimension m and weight $(d_0, ..., d_m)$. Then a*

point $P = (x_0 : ... : x_m) \in \mathbb{P}^{(d_0,...,d_m)}(\overline{k})$ *is* k*-rational if and only if there are* $y_0, ..., y_m \in k^{sep}$ *such that* $P = (y_0 : ... : y_m)$ *and for all* $\sigma \in \mathrm{Gal}(k^{sep}/k)$ *we have* $P = \sigma(P) := (\sigma(y_0) : ... : \sigma(y_m))$.

Proof. Given a k-rational point $P = (x_0 : ... : x_m) \in \mathbb{P}^{(d_0,...,d_m)}(\overline{k})$ with $x_0, ..., x_m \in k$, it is clear that $P = \sigma(P)$ for all $\sigma \in \mathrm{Gal}(k^{\mathrm{sep}}/k)$.

Suppose we have $P = (x_0 : ... : x_m) \in \mathbb{P}^{(d_0,...,d_m)}(\overline{k})$ with $x_0, ..., x_m \in k^{\mathrm{sep}}$ and $\sigma(P) = P$ for all $\sigma \in \mathrm{Gal}(k^{\mathrm{sep}}/k)$. Without loss of generality, we may assume $x_i \neq 0$ for $i = 0, ..., m$, as we can look only at the non-zero coordinates. Also we may assume that $\gcd(d_0, ..., d_m) = 1$, as for weights with common divisor $\gcd(d_0, ..., d_m) = e > 1$ scaling by $\lambda^{1/e}$ for $\lambda \in \overline{k}^*$ corresponds with scaling by λ for weights $d_0/e, d_1/e, ..., d_m/e$.

Let $c_0, ..., c_m \in \mathbb{Z}$ be such that $c_0d_0 + c_1d_1 + ... + c_md_m = 1$. Set $\mu = \prod_{i=0}^m x_i^{c_i}$, so that if we scale the coordinates of P by μ^{-1} we find $P = (\mu^{-d_0}x_0 : ... : \mu^{-d_m}x_m)$. Then we have

$$\prod_{i=0}^m (\mu^{-d_i}x_i)^{c_i} = \prod_{i=0}^m \mu^{-c_id_i} \cdot \prod_{i=0}^m x_i^{c_i} = \mu^{-1} \cdot \mu = 1,$$

hence we may assume that $\prod_{i=0}^m x_i^{c_i} = 1$.

For all $\sigma \in \mathrm{Gal}(k^{\mathrm{sep}}/k)$ we have $\sigma(P) = P$, hence for every $\sigma \in \mathrm{Gal}(k^{\mathrm{sep}})$ we have $\sigma(x_i) = \lambda^{d_i}x_i$ for some $\lambda \in \overline{k}^*$ and all $i = 0, ..., m$. This implies that

$$\begin{aligned} 1 = \sigma(1) = \sigma(\prod_{i=0}^m x_i^{c_i}) = \prod_{i=0}^m \sigma(x_i)^{c_i} = \prod_{i=0}^m (\lambda^{d_i}x_i)^{c_i} \\ = \prod_{i=0}^m \lambda^{c_id_i} \cdot \prod_{i=0}^m x_i^{c_i} = \lambda, \end{aligned}$$

hence $\sigma(x_i) = x_i$ for $i = 0, ..., m$ and all $\sigma \in \mathrm{Gal}(k^{\mathrm{sep}})$. Thus it follows that $x_0, ..., x_m \in k$. □

Our next goal is to establish a map from the space of binary forms to a weighted projective space, by making use of invariants. To have a well-defined map, we need to exclude the (orbits of) forms whose invariants all vanish. As seen before, the discriminant of a binary form is an invariant. The discriminant vanishes whenever the form has a double linear factor, which is a property that indeed remains invariant under linear transformation.

For the binary quadratic f, if k is of characteristic different from 2, the discriminant generates the algebra of invariants, hence all non-constant invariants of f vanish if and only it is the square of a linear factor. For a cubic, this also holds (at least when the characteristic is not 2 or 3): its discriminant generates the algebra of invariants, so that all invariants of the cubic vanish if and only if it has a double linear factor.

A similar result that holds for forms of higher order is given below, whose proof can be found in the notes of Hilbert's lectures. It describes

binary forms for which all invariants vanish; these kind of forms are called *null forms*. This proof assumes the base field to be the complex numbers, but can be generalised to arbitrary fields of characteristic 0. A proof for fields of general characteristic was given by Geyer.

Theorem 2.16 (null form)**.** *Let k be a field and let $\overline{k}$ be an algebraic closure of k. Let $f \in S^n(V)$ be a binary form of degree $n \geq 2$, where we write $n = 2h$ or $n = 2h+1$ for some $h \in \mathbb{Z}$. Then $I(f) = 0$ for all invariants $I \in \mathcal{I}_n(k)$ of positive weight if and only if f has an $(h+1)$-fold linear factor over $\overline{k}$.*

Proof. See [Hil1993, p. 159] for the field of complex numbers and [Gey1974, Folgerung 1, p. 65] for general fields. □

Hence for forms of order $n = 2h$ or $n = 2h+1$, if we consider the set of orbits of forms which do not posses an $h+1$-fold linear factor, we find that there is a map from this set to the weighted projective space corresponding to the invariants generating the algebra $\mathcal{I}_n$.

Corollary 2.17. *Let k be a field and let $\overline{k}$ be an algebraic closure of k. Let $n \geq 2$ be an integer and write $n = 2h$ or $n = 2h+1$. Consider the set $B_n \subset S^n(V)$ of binary forms which do not posses an $h+1$-fold linear factor over $\overline{k}$. Let $I_1, ..., I_l$ be a collection of invariants that generate $\mathcal{I}_n(k)$ and let $w_1, ..., w_l$ be their respective weights. Then there is a map*

$$\begin{aligned} \mathrm{GL}_2(k)\backslash B_n &\to \mathbb{P}^{(w_1,...,w_l)}(k), \\ [f] &\mapsto (I_1(f) : ... : I_l(f)). \end{aligned}$$

Proof. This follows immediately from Theorem 2.16, as it implies that for any binary form f that does not posses an $h+1$-fold linear factor, there must exist some invariant $I \in \mathcal{I}_n(k)$ such that $I(f) \neq 0$. Hence $I_i(f) \neq 0$ for some $i \in \{1, ..., l\}$, so that the map is well-defined. □

Finally, we will describe the image of the map above more precisely. For this, we will consider only the binary forms $B'_n \subset B_n$ which do not posses a $n/2$-fold linear factor. For odd n, this means we have $B_n = B'_n$ and for even n the difference is the forms which posses a linear factor of multiplicity equal to $n/2$.

For algebraically closed fields k, let $\mathrm{Proj}(\mathcal{I}_n(k))$ be the weighted projective variety $\mathbb{V}(J) \subset \mathbb{P}^{(w_1,...,w_l)}(k)$, by letting $\mathcal{I}_n(k) = k[I_1, ..., I_l] = k[X_1, ..., X_l]/J$ where $I_1, ..., I_l$ are non-constant invariants that generate $\mathcal{I}_n(k)$, $X_1, ..., X_l$ are polynomial variables and $J \subsetneq (X_1, ..., X_l)$ is a weighted homogeneous ideal (the ideal of non-trivial relations between these invariants). Then there is a map from the set B'_n of binary forms which do not posses an h-fold linear factor to $\mathrm{Proj}(\mathcal{I}_n(k))$, where $n = 2h$ for n even or $n = 2h-1$ for n odd.

This is the following result by Geyer:

Theorem 2.18. *Let $n \geq 3$ be an integer and write $n = 2h$ or $n = 2h - 1$. Let k be an algebraically closed field. Consider the set $B'_n \subset S^n(V)$ of binary forms which do not posses an h-fold linear factor. Let $\mathcal{I}_n(k)$ denote the algebra of invariants over k. Let $I_1, ..., I_l \in \mathcal{I}_n(k)$ such that $\mathcal{I}_n(k) = k[I_1, ..., I_l]$. Then the map*

$$p : B'_n \to \mathrm{Proj}(\mathcal{I}_n(k)), f \mapsto (I_1(f) : ... : I_l(f))$$

induces a map

$$\pi : \mathrm{GL}_2(k) \backslash B'_n \to \mathrm{Proj}(\mathcal{I}_n(k))$$

that is always injective, surjective if n is odd and leaves out a single point if n is even.

Proof. See [Gey1974, Satz 12, p. 65]. □

In the next chapter, we will look into methods to find, given any point P in the image of π, a representative $f \in B_n$ with these values (up to scaling in the weighted projective space).

3 Reconstruction of forms

In this chapter we will describe a method to reconstruct a binary form from the values of its invariants in fields of general characteristic. It was Mestre [Mes1991] who gave an algorithm to reconstruct binary sextics, for which he used formulae of Clebsch and quadratic covariants of the form. This algorithm is generalized to binary forms of any even degree in an article of Lercier and Ritzenthaler [LR2012], in which it is used to reconstruct hyperelliptic curves of genus $g = 3$.

As these formulae are limited to forms of even degree, we will describe a generic method to reconstruct forms of odd degree, which turns out to be easier. This result is due to Clebsch [Cle1872, Chapter 8] and involves linear covariants. After proving the general result, we will apply it to the case of binary quintics over fields of characteristic 0 or $p > 5$.

This method will allow us, given a point in the corresponding weighted projective space (see Theorem 2.18), to find a representative of the orbit mapping to this point. Moreover, if a form defined over some algebraically closed field k has invariant values that lie in a subfield $l \subset k$, then the resulting form is defined over l.

Throughout this chapter, we will assume k to be a field and $\overline{k}$ to be an algebraic closure of k.

3.1 Transformation by linear covariants

In order to obtain a general form from the values of the invariants, we consider a specific linear transformation of forms using linear covariants. As seen in Proposition 1.9, only forms of odd degree can have non-zero linear covariants, hence the following result is only useful to reconstruct forms of odd degree.

The method is discussed in the book of Clebsch [Cle1872, § 92], where it is used to determine whether one binary form can be transformed into another. Given a general binary form f, it will provide us with a representative of its orbit whose coefficients are quotients of invariants of the form f.

Theorem 3.1. *Let $n \geq 3$ be an integer and let $C_0, C_1 : S^n(V) \to S^1(V)$ be two linearly independent covariants which are of order 1 and respective degrees d_0 and d_1 and weights w_0 and w_1. For $f \in S^n(V)$, view its covariants $C_0(f), C_1(f) \in S^1(V)$ as row vectors (with respect to the basis (x, z)). Define the 2×2 matrix*

$$M_f = \begin{pmatrix} C_0(f) \\ C_1(f) \end{pmatrix},$$

and let $D_f = \det(M_f)$ denote its determinant. Then the map $D_{C_0,C_1} : f \mapsto D_f$ is an invariant of degree $d_0 + d_1$. For any form f such that $D_f \neq 0$, we define $\overline{f} := M_f \cdot f$.

For a general form $h = a_0x^n + a_1x^{n-1}z + ... + a_nz^n$, the coefficient of z^ix^{n-i} in $\overline{h}$ equals $D_h^{-n} \cdot I_i$, where the I_i's are invariants of respective degrees $(n-i)d_1 + id_0 + 1$. We denote these invariants by $I_i^{C_0,C_1}$.

Proof. Let $h = a_0x^n + a_1x^{n-1}z + ... + a_nz^n$ be a general form. As the coordinates of the vectors $C_j(h)$ can be seen as the partial derivatives of the covariants with respect to x and z, it follows that D_h is equal to the first transvectant of C_0 and C_1, hence it is an invariant. From the definition of M_h, it follows immediately that the coefficients of $M_h \cdot h$ are rational functions of the a_i whose denominators divide D_h^n.

In order to prove that the coefficients of $D_h^n \cdot \overline{h}$ are invariants we need to show that, when we apply a linear transformation to the form h, their values change by a power of the determinant of N.

Hence we consider $N \in \mathrm{GL}_2(k)$ and we let $g = N \cdot h$. We can then write $M_h \cdot h = (M_hN^{-1}M_g^{-1}) \cdot (M_g \cdot g)$, so that the linear transformation between $\overline{g}$ and $\overline{h}$ is described by the matrix $M_hN^{-1}M_g^{-1}$. As C_0 and C_1 are covariants, it follows that $(C_j(g))(x,z) = \det(N)^{-w_j} \cdot (N \cdot C_j(h))(x,z)$ for $j = 0, 1$.

Thus we find that

$$M_g = \begin{pmatrix} C_0(g) \\ C_1(g) \end{pmatrix} = \begin{pmatrix} \det(N)^{-w_0} & 0 \\ 0 & \det(N)^{-w_1} \end{pmatrix} \cdot M_h \cdot N^{-1},$$

hence

$$M_hN^{-1}M_g^{-1} = \begin{pmatrix} \det(N)^{w_0} & 0 \\ 0 & \det(N)^{w_1} \end{pmatrix}.$$

So it follows that the transformation of $\overline{h}$ to $\overline{g}$ scales the i-th coefficient by a factor $\det(N)^{-(n-i)w_0-iw_1}$, hence the coefficients are invariants after multiplication by D_h^n.

Finally we can see that $D_h^n \cdot \overline{h} = \sum_{i=0}^n a_i(C_1^z x - C_0^z z)^{n-i}(-C_1^x x + C_0^x z)^i$, where $C_j^x = C_j(1,0)$ and $C_j^z = C_j(0,1)$ for $j = 1, 2$. Thus it follows that the coefficient of x^n is equal to $\sum_{i=0}^n a_i \cdot (C_1^z)^{n-i} \cdot (-C_1^x)^i$, which is of degree $nd_1 + 1$ with respect to $a_0, ..., a_n$ as C_1 is of degree d_1. Similarly it follows that the other invariants are of respective degrees $(n-1)d_1 + d_0 + 1$ up to $nd_0 + 1$. □

This theorem allows us to find a canonical representative for a $\mathrm{GL}_2(\overline{k})$-orbit of binary forms. Given an orbit and a form f in this orbit, if we apply the transformation M_f as above to f, then the coefficients of the resulting form $\overline{f}$ are determined by the orbit up to scaling of the coordinates x and z, which is summarized in the following corollary.

Corollary 3.2. *Let k be a field, $\overline{k}$ an algebraic closure of k, $n \geq 3$ an integer and let $C_0, C_1 : S^n(V) \to S^1(V)$ be two linearly independent covariants which are both of order 1 and of respective weights w_0, w_1. Let $f \in S^n(V)$ a binary*

form such that $D_f \neq 0$ and let $\overline{f} = M_f \cdot f$, with M_f as in Theorem 3.1. Then for every form g in the $\mathrm{GL}_2(k)$-orbit of f, the forms $\overline{f}$ and $\overline{g}$ are the same up to k^*-scaling of the coordinates (x, z).

Proof. Let $f \in S^n(V)$ such that $D_f \neq 0$. Then for any $N \in \mathrm{GL}_2(k)$, if we let $g = N \cdot f$, it follows from the proof of Theorem 3.1 that the transformation of $\overline{f}$ to $\overline{g}$ is given by the matrix $\begin{pmatrix} \det(N)^{w_0} & 0 \\ 0 & \det(N)^{w_1} \end{pmatrix}$. □

If we look at the abstract binary form $\overline{h} = M_h \cdot h$ found in Theorem 3.1, we see that all its coefficients are quotients of two invariants. Therefore, given a form $f \in S^n(V)$ such that $D_f \neq 0$, the coefficients of the form $\overline{f}$ can be computed in terms of the values of the invariants of the form. This yields for every $f \in S^n(V)$ such that $D_f \neq 0$ a $\mathrm{GL}_2(k)$-equivalent form that can be determined solely from the invariant values of f.

Moreover, if we have f and g such that their invariant values are the same up to scaling over k^*, it follows that we can use Theorem 3.1 to show they are $\mathrm{GL}_2(k)$-equivalent. This is the following lemma:

Lemma 3.3. *Let k be an algebraically closed field and let $n \geq 2$ an integer. Let $C_0, C_1 : S^n(V) \to S^1(V)$ be two linearly independent covariants. Let $f \in S^n(V)$ be a binary form such that $D_{C_0,C_1}(f) \neq 0$, with D_{C_0,C_1} as in Theorem 3.1. Let $\{I_1, ..., I_t\} \subset \mathcal{I}_n$ be a set of invariants such that D_{C_0,C_1} and $I_i^{C_0,C_1}$ for $i \in \{0, ..., n\}$ (the invariants as defined in Theorem 3.1) are contained in the subspace $J \subset \mathcal{I}_n$ generated by $\{I_1, ..., I_t\}$.*

Then for $g \in S^n(V)$ such that $I_j(f) = \lambda^{w_j} \cdot I_j(g)$ for some $\lambda \in k^*$ and all $j \in \{1, ..., t\}$, where w_j denotes the weight of I_j, we have that f and g are $\mathrm{GL}_2(k)$-equivalent.

Proof. Let $f, g \in S^n(V)$ and $\lambda \in k^*$ such that $I_j(f) = \lambda^{w_j} \cdot I_j(g)$ for all $j \in \{1, ..., t\}$. Let $M = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Then it follows that $I_j(f) = I_j(M \cdot g)$ for all $j \in \{1, ..., t\}$. Then it follows from Theorem 3.1 that $\overline{f} = \overline{M \cdot g}$, so that it immediately follows that f and g are $\mathrm{GL}_2(k)$-equivalent. □

3.2 Reconstruction of a binary quintic

The main goal of this part will be to prove Theorem 3.10, which describes an explicit inverse of the bijection between the set of $\mathrm{GL}_2(\overline{k})$-orbits of binary quintics and a weighted projective space from Theorem 2.18. This bijection will yield, given a set of values for the invariants A, B and C, a binary quintic attaining these values up to scaling. This process of obtaining a binary form based on invariant values is called *reconstruction of a binary form.*

In order to prove Theorem 3.10, we will use the results from Chapter 2 and the covariants found in 1.3. To use these invariants and covariants, we assume k to be of characteristic 0 or $p > 5$, so all constructions involving

division by integers are well-defined. The methods and coefficients involved were described by Clebsch [Cle1872, § 94], who used similar results to find, given binary forms f and g with invariants equal up to $\mathbb{C}^8$-scaling, an explicit transformation of f to g.

The reconstruction for this case has been implemented as SageMath code by the author as part of the thesis project. After contribution to the SageMath project, it has been peer-reviewed and merged to be part of SageMath version 9.0 and up. The implementation was used by Somoza [Som2019, Section 2.3] to compute, who studied curves of the form $y^5 = xz(x - z)(x - \lambda z)(x - \mu z)$ with $\lambda, \mu \in \overline{\mathbb{Q}}$. Given such a curve, the added functionality was used to compute its invariants, which where contained in $\mathbb{Q}$, and then was used to reconstruct a model over $\mathbb{Q}$ of the curve from these invariants.

3.2.1 General case

Given a binary quintic form $f \in S^5(V)$, for which we know its invariants $A(f)$, $B(f)$ and $C(f)$ (with A, B and C as defined in Table 1), we want to compute a unique representative of its $\mathrm{GL}_2(k)$-orbit using solely the invariants of f. In order to apply Theorem 3.1, we need to find two linearly independent covariants of degree 1.

We can take α and β, so that the corresponding determinant is the invariant $-M$. If we take α and γ, the determinant is equal to $-N$. Thus if we have that $M(f) \neq 0$ or $N(f) \neq 0$, then we can find a general form with the given invariants by making use of the suitable linear covariants and applying Theorem 3.1.

We will list the coefficients of the resulting forms for these cases, which were computed by Clebsch [Cle1872, § 94] and were checked by the author using SageMath [Sage]. A few signs in the book of Clebsch are wrong and were altered by the author to obtain the correct values.

For the general quintic f, write the form $\overline{f}$ obtained from Theorem 3.1 as

$$D^{-5}(A_5x^5 - 5A_4x^4z + 10A_3x^3z^2 - 10A_2x^2z^3 + 5A_1xz^4 - A_0z^5), \qquad (2)$$

where D is the discriminant of the two linear covariants, so that either $D = -M$ or $D = -N$. We can then express the coefficients of $\overline{f}$ in terms of the invariants A, B and C, noting that the values of the invariants M and N can be computed by the relations $M = 2AB - 3C$ and $N = \frac{1}{2}(AC - B^2)$. Finally we make a choice for R using Equation (1) on page 14, which will turn out at most to change the end result $\overline{f}$ into $\overline{f}(-x, z)$.

For the case where α and β are used as coordinates, we obtain the

following coefficients:

$$\begin{aligned}
A_0 &= \frac{1}{3}(2A^2 - 3B)R, \\
A_1 &= \frac{1}{6}(2A^2 - 3B)(AN - BM) + \frac{1}{6}M(2AM - 3N), \\
A_2 &= MR - \frac{1}{2}A \cdot A_0, \\
A_3 &= \frac{1}{2}M(AN - BM) - \frac{1}{2}A \cdot A_1, \\
A_4 &= -AMR + \frac{1}{4}A^2 \cdot A_0, \\
A_5 &= -M^3 - \frac{1}{2}AM(AN - BM) + \frac{1}{4}A^2 \cdot A_1.
\end{aligned} \tag{3}$$

For the case where α and γ are used as coordinates, we obtain the following coefficients:

$$\begin{aligned}
A_0 &= \frac{1}{3}(2A^2 - 3B)R, \\
A_1 &= \frac{1}{6}(2A^2 - 3B)(BN - CM) - \frac{1}{6}N(3N - 2AM), \\
A_2 &= \frac{2}{3}ANR - \frac{1}{2}C \cdot A_0, \\
A_3 &= \frac{1}{3}AN(BN - CM) + \frac{1}{3}MN^2 - \frac{1}{2}C \cdot A_1, \\
A_4 &= \frac{2}{3}N^2R - \frac{2}{3}ACNR + \frac{1}{4}C^2 \cdot A_0, \\
A_5 &= BN^3 - \frac{1}{3}CMN^2 - \frac{1}{3}ABCN^2 + \frac{1}{4}C^2 \cdot A_1.
\end{aligned} \tag{4}$$

Remark 3.4. *The method above can be generalised to binary forms of higher odd degree $n = 2h + 1$. We can define a quadratic covariant $\psi = (f, f)_{2h}$ (of degree 2), then use this to define a first linear covariant $\alpha = (\psi^h, f)_{2h}$ (of degree $2h + 1 = n$). A second linear covariant is the transvectant of the first linear covariant with the quadratic covariant, i.e. $\beta = (\psi, \alpha)_1$ (of degree $2h + 3 = n + 2$). Their corresponding determinant D is an invariant of degree $2n + 2$ and all forms for which this invariant do not vanish can be transformed using these covariants. Note that these definitions of α and β coincide with the ones given in Table 1 for binary quintics.*

It can be shown that this invariant is non-zero for fields of characteristic 0 by computing $D(x^h z^h(x + z))$, which is non-zero for $h \geq 1$: we have $\psi(x^h z^h(x + z)) = c_0(x^2 + \frac{2}{h+1}xz + z^2)$ for some $c_0 \in \mathbb{Q}$, so that $\alpha(x^h z^h(x + z)) = c_1(x + z)$ and $\beta(x^h z^h(x + z)) = c_2(x - z)$ for some $c_1, c_2 \in \mathbb{Q}$.

In order to reconstruct forms for which this invariant does vanish, a closer study of the algebra of covariants of degree n is required.

From Equation (1) it follows that R vanishes if both M and N do for a binary quintic f. In this case the determinants of all the 6 possible pairs of linear covariants found in Section 1.3 vanish, as they are respectively $-N$, $-M$, R, $-R$, $\frac{1}{2}(NA-MB)$ and $\frac{1}{2}(NB-MC)$ (see also [Cle1872, p. 280]).

Therefore a linear transformation with covariants cannot be used to reconstruct a form in terms of the invariants if both M and N vanish. However, there are only finitely many $\mathrm{GL}_2(\overline{k})$-orbits for which this happens, as we will see in subsection 3.2.2.

For a form $f \in S^5(V)$ for which $M(f) \neq 0$ or $N(f) \neq 0$, the coefficients of the forms described above are uniquely determined by the values of the invariants of f. For any form g that is $\mathrm{GL}_2(k)$-equivalent to f, it follows from Corollary 3.2 that $\overline{f}$ and $\overline{g}$ for the same choice of linear covariants (as defined in Theorem 3.1) are the same up to scaling of the coordinates.

In order to reconstruct a form that no longer depends on the choice of f in a $\mathrm{GL}_2(\overline{k})$-orbit, we want to find a form such that all coefficients are *absolute invariants*: quotients of two invariants of the same degree. We will call such a form a *canonical form*: this is a chosen representative f in the orbit such that its coefficients are determined in terms of the values of absolute invariants. Moreover, the coefficients of the chosen forms will be rational functions of the invariants, hence if a form has invariant values in some field $l \subset \overline{k}$, the canonical form will be defined over l.

For the case where $M(f) \neq 0$ or $N(f) \neq 0$, the canonical form is given by the lemma below. The other cases are listed in Lemma 3.6.

Lemma 3.5 (canonical form)**.** *Let k be a field of characteristic 0 or $p > 5$. Let $A, B, C \in k$ such that $M = 2AB - 3C \neq 0$ or $N = \frac{1}{2}(AC - B^2) \neq 0$. Choose $R \in \overline{k}$ such that it satisfies Equation (1) (on page 14) and let $\tilde{f}$ be a quintic over $\overline{k}$ given by the following:*

(a) if $M \neq 0$, $R \neq 0$ and $A \neq 0$, then $\tilde{f} = M^2 \cdot (Q \cdot f_0)$, with f_0 defined by formulas (2) and (3) and where

$$Q = \begin{pmatrix} 1 & 0 \\ 0 & R^{-1}A^4 \end{pmatrix};$$

(b) if $M \neq 0$, $R \neq 0$, $A = 0$ and $B \neq 0$, then $\tilde{f} = M^2 \cdot (Q \cdot f_0)$, with f_0 defined by formulas (2) and (3) and where

$$Q = \begin{pmatrix} 1 & 0 \\ 0 & R^{-1}B^2 \end{pmatrix};$$

(c) if $M \neq 0$, $R \neq 0$ and $A = B = 0$, then $\tilde{f} = x^5 + x^2z^3$;

(d) *if* $M \neq 0$, $R = 0$ *and* $A \neq 0$, *then* $\tilde{f} = A^{11} \cdot (Q \cdot f_0)$, *with* f_0 *defined by formulas* (2) *and* (3) *and where*

$$Q = \begin{pmatrix} A & 0 \\ 0 & A^{1/2} \end{pmatrix},$$

for any choice of $A^{1/2}$;

(e) *if* $M \neq 0$ *and* $R = A = 0$, *then* $\tilde{f} = x^5 + 10x^3z^2 - 15xz^4$;

(f) *if* $M = 0$ *and* $A \neq 0$, *then* $\tilde{f} = A^6 \cdot (Q \cdot f_0)$, *with* f_0 *defined by formulas* (2) *and* (4) *and where*

$$Q = \begin{pmatrix} 1 & 0 \\ 0 & R^{-1}A^3 \end{pmatrix};$$

(g) *if* $M = A = 0$, *then* $\tilde{f} = x^5 + xz^4$.

Then $\tilde{f}$ *has coefficients in* k, *is independent of the choices of roots for* R^2 *and* A *and there is* $\alpha \in \overline{k}^*$ *such that* $(A, B, C) = (\alpha \cdot A(\tilde{f}), \alpha^2 \cdot B(\tilde{f}), \alpha^3 \cdot C(\tilde{f}))$. *Moreover, if we have* $f \in S^5(V)$ *and* $\beta \in \overline{k}^*$ *such that* $(A, B, C) = (\beta \cdot A(f), \beta^2 \cdot B(f), \beta^3 \cdot C(f))$, *then* $f \in \mathrm{GL}_2(\overline{k})\tilde{f}$.

Proof. First let us note that a different choice for a root of A in case *(d)* does not change $\tilde{f}$: as $R = 0$, it follows all the terms A_i with i even vanish. So only the odd terms remain, which all correspond to an even power of z, so that no square roots of A remain in the coefficients of $\tilde{f}$. Similarly, a different choice of R based on Equation (1) in the cases *(a)*, *(b)* and *(f)* does not change $\tilde{f}$ in these cases, as the transformation multiplies all A_i with i even by an odd power of R and all A_i with i odd by an even power of R, so that in the resulting form $\tilde{f}$ only even powers of R appear in the coefficients.

Hence for the forms listed above, it is clear that the coefficients of $\tilde{f}$ are rational functions of the invariants A, B and C in all cases (as we can replace R^2 using Equation (1)), hence $\tilde{f}$ is defined over k. We will now show for each of the listed cases, the chosen form $\tilde{f}$ has the correct invariant values.

In the case where $M \neq 0$, we use formulas (2) and (3) (corresponding with using linear covariants α and β as coordinates). Then we see that the invariants A_0, A_1, ..., A_5 are of respective degrees 26, 28, ..., 36 and $D^{-5} = (-M)^{-5}$ is of degree 60. We consider two cases, based on the vanishing of the invariant R.

If we have $R \neq 0$, we consider the following cases:

(a) if $A \neq 0$, we can apply the linear transformation replacing z by $RA^{-4}z$, so that the resulting A_i's are all of degree 36. If we multiply the form by M^2 and take into account the factor $D^{-5} = -M^{-5}$, the resulting form has absolute invariants as coefficients;

(b) if $B \neq 0$, we can apply the linear transformation replacing z by $RB^{-2}z$ and obtain, in a similar way to the case above, a form whose coefficients are absolute invariants;

(c) in the case $A = B = 0$, one can see from Equation (3) that all coefficients except A_2 and A_5 vanish. Therefore, after suitable scaling, it follows that the form is $\mathrm{GL}_2(\overline{k})$-equivalent to $x^5 + x^2z^3 = x^2(x^3 + z^3)$.

If the invariant R vanishes, one can see from Equation (3) that $A_0 = A_2 = A_4 = 0$ in this case. We can then look at the value of A to find the canonical form:

(d) if $A \neq 0$ we can apply a linear transformation replacing x by $A^{-1}x$ and z by $A^{-1/2}z$. As A is of degree 4, the respective degrees of the new A_i's are all equal to 16 after this transformation. So if we multiply the form by A^{11} and take into account the factor $D^{-5} = -M^{-5}$ of degree $5 \cdot 12 = 60$, it follows that the resulting form has absolute invariants as coefficients;

(e) if $A = 0$, we obtain the form $x^5 + 10x^3z^2 - 15xz^4$ after scaling.

Finally in the case where $M = 0$ and $N \neq 0$, we use the formulas (2) and (4). From this we can deduce that the invariants A_0, A_1, ..., A_5 are of respective degrees 26, 32, ..., 56. As M vanishes, we have $R^2 = -\frac{1}{2}AN^2$, so that R vanishes if and only if A does, so we have two cases:

(f) if A and R do not vanish, we can apply the linear transformation replacing z by $RA^{-3}z$, so that the resulting A_i's are all of degree 56. If we multiply the form by A^6 and take into account the factor $D^{-5} = -N^{-5}$ of weight $5 \cdot 16 = 80$, the resulting form has absolute invariants as coefficients.

(g) if $A = R = 0$, it follows that all coefficients but A_1 and A_5 vanish, so that after a suitable linear transformation the form is equal to $x(x^4 + z^4)$.

To prove that $\tilde{f}$ is indeed $\mathrm{GL}_2(\overline{k})$-equivalent to f if $(A(f), B(f), C(f)) = (\alpha \cdot A(\tilde{f}), \alpha^2 \cdot B(\tilde{f}), \alpha^3 \cdot C(\tilde{f}))$ for some $\alpha \in k$, we can apply Lemma 3.3. □

3.2.2 Special cases

In subsection 3.2.1 we have reconstructed binary quintics $f \in S^5(V)$ whose invariants satisfy $M(f) \neq 0$ or $N(f) \neq 0$. We need a different method for the case where both M and N vanish. Clebsch [Cle1872, § 93] gave explicit computations for this case, where he used covariants to compute the possible forms f having the given invariants.

Lemma 3.6 (canonical form (continued from Lemma 3.5))**.** *Let k be a field of characteristic 0 or $p > 5$. Let $A, B, C \in k$ such that $A \neq 0$, $M = 2AB - 3C = 0$ and $N = \frac{1}{2}(AC - B^2) = 0$. Let $\tilde{f} \in S^5(V)$ be given by the following:*

(h) $\tilde{f} = x^4z + xz^4$ *if* $A \neq 0$ *and* $B \neq 0$*;*

(i) $\tilde{f} = x^5 + z^5$ *if* $A \neq 0$ *and* $B = C = 0$*.*

Then there is $\alpha \in \overline{k}^*$ *such that* $(A, B, C) = (\alpha \cdot A(\tilde{f}), \alpha^2 \cdot B(\tilde{f}), \alpha^3 \cdot C(\tilde{f}))$*. Moreover, if we have* $f \in S^5(V)$ *and* $\beta \in \overline{k}^*$ *such that* $(A, B, C) = (\beta \cdot A(f), \beta^2 \cdot B(f), \beta^3 \cdot C(f))$*, then* $f \in \mathrm{GL}_2(\overline{k})\tilde{f}$*.*

Proof. First we note that the vanishing of M and N implies we have the relations $2AB = 3C$ and $AC = B^2$ between the invariants of the form (see Section 1.3). If we consider the case where A does not vanish, without loss of generality, we can scale such that we have $A = 3$ and obtain the relations $6B = 3C$ and $3C = B^2$. This yields two possible solutions, namely the case $B = C = 0$ and the case $B = 6$ and $C = 12$.

In both cases it is straightforward to verify that $\tilde{f}$ has the correct invariant values (up to scaling). So it remains to show that given f with these invariants up to scaling, it follows that $f \in \mathrm{GL}_2(\overline{k})\tilde{f}$.

First we note that the assumption $A(f) \neq 0$ is equivalent to the quadratic covariant $i(f)$ not being a square in $\overline{k}[x, z]$, as the discriminant of i is equal to $-2A$. Clebsch uses this fact by choosing the two linear factors $\xi, \eta \in \overline{k}[x, z]$ of i to be the coordinates of f. After applying the corresponding transformation, we have $f = a\xi^5 + b\xi^4\eta + c\xi^3\eta^2 + d\xi^2\eta^3 + e\xi\eta^4 + g\eta^5$ for some $a, b, c, d, e, g \in \overline{k}$. Note that while Clebsch assumed the base field to be $k = \mathbb{C}$, all the computations remain valid over $\overline{k}$ for any field k of characteristic 0 or $p > 5$.

(h) *The case where both A and B do not vanish,*
i.e. $(A : B : C) = (3 : 6 : 12) \in \mathbb{P}^{(1,2,3)}(k)$
This case corresponds to case I in the book of Clebsch [Cle1872, § 93, p. 370-371]. There it is shown that if f is written in terms of ξ and η as above, it follows that in this case we have $a = c = d = g = 0$. So it follows that f is of the form $f = \xi\eta(b\xi^3 + e\eta^3)$, hence it is $\mathrm{GL}_2(\overline{k})$ equivalent to $\tilde{f} = xz(x^3 + z^3)$.

(i) *The case $A \neq 0$ and $B = C = 0$*
This case is case III [Cle1872, § 93, p. 373-374] in Clebsch' book. There, Clebsch shows that if we use the linear factors ξ, η of i to be the coordinates, then f is the sum of the fifth powers of these factors (up to scaling). Hence it follows that f is $\mathrm{GL}_2(\overline{k})$-equivalent to $\tilde{f} = x^5 + z^5$.

□

Finally we have to consider the case where the invariants A, B, C all vanish for $f \in S^5(V)$. We will show that in this case, f is actually a null form, hence all its invariants vanish. Note that our proof relies on explicit computation, if one would show that $\{A, B, C\} \subset \mathcal{I}_5(k)$ is a separating subset this result would follow almost immediately from that fact.

Lemma 3.7. *Let k be a field of characteristic 0 or $p > 5$. Let $f \in S^5(V)$ be a quintic such that $A(f) = B(f) = C(f) = 0$. Then f is a null form.*

Proof. First we note that Theorem 2.16 implies that proving this claim is equivalent to proving that f has a threefold linear factor over $\overline{k}$. Now suppose that we have $f \in S^5(V)$ such that $A(f) = B(f) = C(f) = 0$, but f has no threefold linear factor. Then f has at least three distinct linear factors.

As $A(f) = B(f) = C(f) = 0$, it follows that the discriminant Δ of f is 0 as we have $\Delta = 5^5 \cdot \frac{A^2 - 64B}{4}$, hence f has a twofold linear factor. So after a suitable transformation of coordinates, we have $f = x^2z(x + z)(x + \lambda z)$ for some $\lambda \in \overline{k}^*$. Then we find that we have $A(f) = \frac{4}{5^4}\lambda^2(\lambda^2 - \lambda + 1)$ and $C(f) = -\frac{3}{2^5 \cdot 5^{12}}\lambda^6(4\lambda^6 - 12\lambda^5 - \lambda^4 + 22\lambda^3 - \lambda^2 - 12\lambda + 1)$. If we consider $A(f) \cdot \lambda^{-2}$ and $C(f) \cdot \lambda^{-6}$ as polynomials in terms of λ, we can compute their resultant and find that it is equal to $2^2 \cdot 3^2 \cdot 5^{-44}$. Thus it follows that there is no $\lambda \in \overline{k}^*$ such that $A(f) = C(f) = 0$.

Thus we find that f must have a threefold linear factor, hence is a null form. □

3.2.3 Canonical form

The lemmas 3.5 and 3.6 now allow us to define a canonical form for any $f \in S^5(V)$ that does not posses a threefold linear factor, i.e. f is not a null form.

Definition 3.8 (canonical form)**.** *Let $f \in S^5(V)$ be a binary form that is not a null form. Let $\tilde{f} \in S^5(V)$ be the form corresponding to $(A(f), B(f), C(f))$ as defined in Lemma 3.5 or Lemma 3.6. Then $\tilde{f}$ is called the* canonical form *of f.*

Remark 3.9. *Null forms $f \in S^5(V)$ cannot be distinguished in terms of invariants, as they all vanish. Still a canonical form can be defined by looking at the multiplicities of the linear factors, as such a form can have at most 3 distinct factors. Thus up to $\mathrm{GL}_2(\overline{k})$-equivalence, we are left with 4 possibilities, namely $f = x^3z(x + z)$ (a threefold linear factor together with two distinct linear factors), $f = x^3z^2$ (a threefold linear factor together with a twofold linear factor), $f = x^4z$ and $f = x^5$.*

3.2.4 Bijection with the space $\mathbb{P}^{(1,2,3)}(k)$

We now combine the results from lemmas 3.5 and 3.6 to establish an explicit inverse of the map between $\mathrm{GL}_2(k)$-orbits of forms and points in the weighted projective space from Theorem 2.18, as follows:

Theorem 3.10. *Let k be an algebraically closed field of characteristic 0 or $p > 5$. Let $B_5 \subset S^5(V)$ denote the space of binary quintic forms over k which do not posses a threefold linear factor. Let A, B and C be as in Table 1. Then there is a bijection*

$$\begin{aligned} \mathrm{GL}_2(k)\backslash B_5 &\to \mathbb{P}^{(1,2,3)}(k), \\ [f] &\mapsto (A(f), B(f), C(f)). \end{aligned}$$

Moreover, the inverse is explicit in the sense that it maps $(a : b : c) \in \mathbb{P}^{(1,2,3)}(k)$ to $\tilde{f}$ as described by Lemma 3.5 or Lemma 3.6. This inverse maps points defined over any subfield $l \subset k$ to quintics $\tilde{f}$ with coefficients in l.

Proof. First we note that the map is well-defined, as from Lemma 3.7 it follows that $A(f) = B(f) = C(f) = 0$ implies that f has a threefold linear factor, and A, B and C are invariants whose respective weights scale by a $1 : 2 : 3$ ratio.

Then injectivity and surjectivity follow from lemmas 3.5 and 3.6, and also the claim about the coefficients of f in l follows immediately from these lemmas. □

3.2.5 Reconstruction in SageMath

The author's implementation of these invariants in SageMath is part of version 9.0 and later; see https://trac.sagemath.org/ticket/25508. An example of the functionality can be found below. This implementation is part of the thesis work.

Example 3.11 (Reconstruction of binary quintics in SageMath)**.**

```
""" For fields of characteristic 0 or characteristic greater than 5,
    binary quintics can be reconstructed using the
    invariant_theory.binary_form_from_invariants function in Sage.
    This can be done by providing a tuple or list of invariants."""

sage: invariants = [2, 6, 8]
sage: quintic = invariant_theory.binary_form_from_invariants(5, invariants)
sage: quintic
Binary quintic with coefficients (1000000000000000/3, -2500000000000000000,
0, 2000000000000000000000000, -6000000000000000000000000000,
8400000000000000000000000000000)

""" The function also allows scaling by the gcd if possible."""

sage: invariants = [2, 6, 8]
```

```
sage: quintic = invariant_theory.binary_form_from_invariants(5, invariants, \
                                                             scaling='coprime')
sage: quintic
Binary quintic with coefficients (1, -7500, 0, 60000000000,
-180000000000000, 252000000000000000)

""" It is also possible to compute the canonical form of a
    binary quintic. Note the form computed in this example
    is not the canonical form as defined previously, but has
    its coefficients scaled for readability."""

sage: R.<x0, x1> = QQ[]
sage: p = 3*x1^5 + 6*x1^4*x0 + 3*x1^3*x0^2 + 4*x1^2*x0^3 - 5*x1*x0^4 + 4*x0^5
sage: f = invariant_theory.binary_quintic(p, x0, x1)
sage: f.canonical_form(reduce_gcd=True)
Binary quintic with coefficients (2707431522222163101550,
121328440685285415859314 81, 25176044506195873425919275600,
22155751009391231173323649389984, 11705410975362392714725242546566400,
21742037117931421324406167187193 19296)
sage: g = matrix(QQ, [[11,5],[7,2]])
sage: gf = f.transformed(g)
sage: f.canonical_form() == gf.canonical_form()
True
```

4 Binary quintics over fields of small characteristic

To conclude this thesis, we will apply the results from the previous two chapters to describe the invariants of binary quintics over fields k of characteristic 2, 3 and 5. We will give a reconstruction of binary quintics for those fields, to find a representative of the orbit given a tuple of invariant values. For a tuple with values that lie in a subfield $l \subset k$, the resulting form is defined over l, except in a certain case where the characteristic of k is 2 (see Theorem 4.5).

Throughout this chapter, we will assume k to be a field and $\overline{k}$ to be an algebraic closure of k.

4.1 Invariants of binary quintics

We will first determine the invariants of binary quintics for fields is of small positive characteristic p. We start with the set of arithmetic invariants found in Section 1.3.2 and try to extend this set to find a full set of generators. For the case $p = 2$ such a set was already found by Du Plessis and Wall [dPW2018], for the other cases we use the set of arithmetic invariants to reconstruct the quintics. The resulting form is unique for characteristic 3 and unique in almost all cases for characteristic 5.

4.1.1 Fields of characteristic 2

For fields of characteristic 2, the set of generators for the algebra $\mathcal{I}_5$ has an 'additional' generator when compared to the case of the complex numbers. This is the following result.

Proposition 4.1 (Du Plessis and Wall)**.** *Let k be a field of characteristic 2. Then the algebra $\mathcal{I}_5(k)$ is generated by i_4, i_6 and i_8, where i_4 and i_8 are the reductions modulo 2 of respectively I_4 and I_8 and where $i_6^2 = i_{12}$, where i_{12} is the reduction of I_{12} modulo 2. Moreover, there is no non-trivial relation between these invariants.*

Proof. This follows immediately from [dPW2018, Theorem 6.2, p. 12]. Note that while the definitions of I_4, I_8 and I_{12} we use differ from those in that article, the invariants i_4, i_6 and i_8 we obtain are exactly the same as the ones in the article. □

Remark 4.2. *Where in the case of the complex numbers we have another generator I_{18}, this is not the case in characteristic 2. If we let i_{18} be the reduction modulo 2 of I_{18}, we find that we have $i_{18} = i_6^3$.*

4.1.2 Fields of characteristic 3 and 5

For fields of characteristic $p = 3$ or $p = 5$, no full description of the algebra of invariants will be given in this thesis. We do however find a subalgebra

$k[i_4, i_8, i_{12}, i_{18}] \subset \mathcal{I}_5(k)$ in these cases, where i_4, i_8, i_{12} and i_{18} are the reductions modulo p of respectively I_4, I_8, I_{12} and I_{18}. This subalgebra suffices for our purpose of reconstructing binary quintics.

The reduction of the syzygy in (1) in characteristic 3 is given by

$$i_{18}^2 = -i_4^9 - i_4^7 i_8 + i_4^6 i_{12} + i_4^4 i_8 i_{12} - i_4^3 i_8^3 - i_4^3 i_{12}^2 - i_4^2 i_8^2 i_{12} - i_4 i_8^4 - i_8^3 i_{12}. \quad (5)$$

and in characteristic 5 by

$$i_{18}^2 = -(i_4^9 + i_4^7 i_8 + 2i_4^6 i_{12} + i_4^5 i_8^2 + i_4^4 i_8 i_{12} - 2i_{12}^3). \quad (6)$$

Remark 4.3. *In theory a computation with MAGMA, similar to the computation of a separating subset of the algebra of covariants for quartics in characteristic $p = 3$ done by Rovetta [Rov2017, Appendix A], should yield a separating subset of the algebra of invariants in these cases. However, in practice our attempt did not finish within reasonable time (< 7 days).*

4.2 Reconstruction for fields of small characteristic

In this section we will reconstruct binary quintics over fields k of positive characteristic $p \leq 5$. As seen in the previous section, for these fields the reduction modulo p of the set of generators of the algebra of invariants over $\mathbb{Z}$ does not necessarily generate the algebra of invariants over k.

Yet we can still apply Theorem 3.1: if we consider the linear covariants in Table 2 as polynomials over $\mathbb{Z}$, then we can consider their reduction modulo p. The linear covariants obtained in this way can then be used as coordinates to obtain a corresponding linear transformation.

4.2.1 Characteristic 2

Consider a field k of characteristic 2. As seen in 4.1.1 the algebra of invariants $\mathcal{I}_5(k)$ is generated by the invariants i_4, i_6 and i_8. If we reduce α' and β' (see Table 2) modulo 2, then we find that:

$$\overline{\alpha'} = (a_2^2 a_3^3 + a_1 a_3^4 + a_2^4 a_5)x + (a_2^3 a_3^2 + a_0 a_3^4 + a_2^4 a_4)z$$
$$\overline{\beta'} = i_6 \cdot (a_2 x + a_3 z).$$

Hence we can use the covariants $\alpha_2 = \overline{\alpha'}$ and $\beta_2 = a_2 x + a_3 z$ as coordinates when their determinant does not vanish. Their determinant is the invariant i_6 and we find that for a quintic f with $i_6(f) \neq 0$ the corresponding transformed form is

$$i_6^5 \overline{f} = A_0 x^5 + A_3 x^2 z^3 + A_4 x z^4 + A_5 z^5, \quad (7)$$

where

$$A_0 = i_6 \qquad A_4 = i_6(i_8^2 + i_4 i_6^2)$$
$$A_3 = i_6^3 \qquad A_5 = i_6^3 i_8.$$

So given a set of values for the invariants i_4, i_6 and i_8, where i_6 has non-zero value, we can use this to reconstruct a binary quintic with the corresponding values for the invariants up to scaling. To find a representative for the cases where i_6 vanishes, we use the following theorem from Du Plessis and Wall on binary quintics over fields of characteristic 2.

Theorem 4.4 (special case reconstruction)**.** *Let k be an algebraically closed field of characteristic 2. A binary quintic $f \in S^n(V)$ with $i_6(f) = 0$ and with $i_4(f) \neq 0$ or $i_8(f) \neq 0$ is $\mathrm{GL}_2(k)$-equivalent to one of the following forms:*

1. *if $i_4(f) \neq 0$ and $i_8(f) \neq 0$, then f is equivalent to the form $g(x, z) = a_1x^4z + x^2z^3 + a_4xz^4$ with $a_1 \neq 0$, $a_4 \neq 0$ and invariants $i_4(f) = a_1^2a_4^2$ and $i_8(f) = a_1^2$;*
2. *if $i_8(f) = 0$ (and $i_4(f) \neq 0$), then f is equivalent to the form x^4z+xz^4;*
3. *if $i_4(f) = 0$ (and $i_8(f) \neq 0$), then f is equivalent to the form $x^3z^2+xz^4$.*

Proof. The first two cases above correspond with case (b) of Theorem 6.1 in the article of Du Plessis and Wall [dPW2018, p. 11]. This theorem claims that a form f with $i_4(f) \neq 0$ and $i_6(f) = 0$ is $\mathrm{SL}_2(k)$-equivalent to a unique (normal) form $g(x, z) = a_1x^4z + a_3x^2z^3 + a_4xz^4$ with $a_1 \neq 0$, $a_4 \neq 0$ and invariants $i_4(f) = i_4(g) = a_1^2a_4^2$ and $i_8(f) = i_8(g) = a_1^2a_3^6$, where either $a_3 = 1$ or $a_3 = 0$, $a_1 = 1$.

In case (a) we have $i_8(f) \neq 0$ and hence $a_3 \neq 0$, thus it follows that $a_3 = 1$ in this case. For case (b) the assumption $i_8(f) = 0$ implies $a_3 = 0$ and $a_1 = 1$, hence f is $\mathrm{SL}_2(k)$ equivalent to $x^4z + a_4xz^4$ with $a_4 \neq 0$, which is $\mathrm{GL}_2(k)$-equivalent to $x^4z + xz^4$.

The last case corresponds to part (c) of the same theorem, which claims that a form f with $i_4(f) = 0$ and $(i_6(f), i_8(f)) \neq (0, 0)$ is $\mathrm{SL}_2(k)$-equivalent to the form $g(x, z) = x^3z^2 + a_4xz^4 + a_5z^5$ where $i_6(f) = i_6(g) = a_5$ and $i_8(f) = i_8(g) = a_4^2$. As $i_6(f) = 0$ we find that $g(x, z) = x^3z^2 + a_4xz^4$ with $a_4 \neq 0$, which is $\mathrm{GL}_2(k)$-equivalent to $x^3z^2 + xz^4$. □

The transformed form from Equation (7) and Theorem 4.4 together allow us to reconstruct a binary quintic for any tuple of invariant values, which leads to the following theorem.

Theorem 4.5. *Let k be an algebraically closed field of characteristic 2. Let $B_5 \subset S^5(V)$ denote the space of binary quintic forms over k which do not posses a threefold linear factor. Then there is a bijection*

$$\begin{aligned} \mathrm{GL}_2(k)\backslash B_5 &\to \mathbb{P}^{(2,3,4)}(k), \\ [f] &\mapsto (i_4(f) : i_6(f) : i_8(f)). \end{aligned}$$

Moreover, if $(i_4 : i_6 : i_8) \in \mathbb{P}^{(2,3,4)}(k)$ is a point defined over some field l such that $l \subset k$, then there exists a quintic f in the corresponding orbit with

coefficients in a quadratic extension of l. If $i_6 \neq 0$ or l is perfect, then there exists a quintic f in the corresponding orbit which is defined over l.

Proof. First we note the map is well-defined, as by Proposition 4.1 the algebra $\mathcal{I}_5(k)$ is generated by i_4, i_6 and i_8, so that $i_4(f) = i_6(f) = i_8(f) = 0$ implies that $i(f) = 0$ for all invariants $i \in \mathcal{I}_5(k)$ of positive weight. Thus in that case f is a null form and Theorem 2.16 gives a contradiction with $f \in B_5$.

For the case $i_6 \neq 0$, the surjectivity follows from the fact that the form $f = A_0x^5 + A_3x^2z^3 + A_4xz^4 + A_5z^5$ as defined in (7) is a form with the correct invariants. Moreover, if we have two forms mapping to the same point $(i_4 : i_6 : i_8) \in \mathbb{P}^{(2,3,4)}(k)$ with $i_6 \neq 0$, then they are $\mathrm{GL}_2(k)$-equivalent by Lemma 3.3. For $(i_4 : i_6 : i_8) \in \mathbb{P}^{(2,3,4)}(l)$ with $l \subset k$ it is clear that f has coefficients in l.

Suppose we have a point $(i_4 : i_6 : i_8) \in \mathbb{P}^{(2,3,4)}(k)$ such that $i_6 = 0$. If $i_8 = 0$, it follows from Theorem 4.4 that $f = x^4z + xz^4$ has the correct invariants and any form g with invariants $(0 : 0 : 1)$ is equivalent to f; similarly when $i_6 = 0$ we can use the form $x^3z^2 + xz^4$. It is also clear these forms are defined over any subfield $l \subset k$.

If $i_6 = 0$ and $i_4, i_8 \in k^*$, we consider the form $f = a_1x^4z + x^2z^3 + a_4xz^4$ where a_1 and a_4 are defined by $a_1 = \sqrt{i_8}$ and $a_4 = \sqrt{i_4i_8^{-1}}$ (which defines them uniquely as k is of characteristic 2). Then Theorem 4.4 tells us that f has the correct invariants and moreover any g having the same invariants up to scaling will be $\mathrm{GL}_2(k)$-equivalent to f.

Now suppose we have $i_4, i_8 \in l^*$ for some subfield $l \subset k$. Without loss of generality, we may assume that i_4 is a square in l (as we have $(i_4 : 0 : i_8) = (i_4^2 : 0 : i_4^2i_8)$). So it follows that the form $f = a_1x^4z + x^2z^3 + a_4xz^4$ has coefficients in l if and only if i_8 is a square in l.

So we can conclude that for a point $(i_4 : i_6 : i_8)$ defined over some field l, the quintic as described above is defined over l if $i_6 \neq 0$ or if i_8 is a square in l. When l is perfect, the latter is always satisfied, hence the quintic is defined over l in this case. □

4.2.2 Characteristic 3

Consider a field k of characteristic 3. As seen in 4.1.2, there is a subalgebra of the algebra of invariants $\mathcal{I}_5(k)$ generated by the invariants i_4, i_8, i_{12} and i_{18}. If we reduce α' and β' (see Table 2) modulo 3, then we find that $\overline{\beta'}$ is given by:

$$\begin{aligned}\overline{\beta'} = i_4 \cdot \big((&a_0a_3a_5 - a_0a_4^2 + a_1a_2a_5 + a_1a_3a_4 - a_2a_3^2 - a_2^2a_4)x \\ &- (a_0a_3a_4 + a_0a_2a_5 + a_1a_2a_4 - a_1a_3^2 - a_1^2a_5 - a_2^2a_3)z\big).\end{aligned}$$

Hence we can use the covariants $\alpha_3 = \overline{\alpha'}$ and $\beta_3 = \frac{\overline{\beta'}}{i_4}$ as coordinates. Their determinant is the invariant $-i_8$ and we find that for a quintic f with

$i_8(f) \neq 0$ the corresponding transformed form is

$$-i_8^5 \overline{f} = A_0 x^5 + A_1 x^4 z + A_2 x^3 z^2 + A_3 x^2 z^3 + A_4 x z^4 + A_5 z^5, \tag{8}$$

where

$$\begin{aligned} A_0 &= i_4^2 i_{18} & A_3 &= -i_4 i_8^2 - i_4^2 i_{12} \\ A_1 &= -i_4^2 i_8^2 - i_4^3 i_{12} + i_8^3 & A_4 &= -i_{18} \\ A_2 &= -i_4 i_{18} & A_5 &= i_8^2 + i_4 i_{12}. \end{aligned}$$

So given a set of values for the invariants i_4, i_8 and i_{12}, where i_8 has non-zero value, we can use this to reconstruct a binary quintic with the corresponding values for the invariants up to scaling.

In order to construct a well-defined map $\mathrm{GL}_2(k)\backslash B_5 \to \mathbb{P}^{(1,2,3)}(k)$, we first need to show that if i_4, i_8 and i_{12} all vanish for a binary quintic f, then f is a null-form, similar to Lemma 3.7.

Lemma 4.6. *Let k be a field of characteristic $p = 3$ or $p = 5$. Let i_4, i_8 and i_{12} be the reductions modulo p of respectively I_4, I_8 and I_{12} (as defined in Table 2). Let $f \in S^5(V)$ be a quintic such that $i_4(f) = i_8(f) = i_{12}(f) = 0$. Then f is a null form.*

Proof. First we note that Theorem 2.16 implies that proving this claim is equivalent to proving that f has a threefold linear factor over $\overline{k}$. Now suppose that we have $f \in S^5(V)$ such that $i_4(f) = i_8(f) = i_{12}(f) = 0$, but f has no threefold linear factor. Then f has at least three distinct linear factors.

As $i_4(f) = i_8(f) = i_{12}(f) = 0$, it follows that the discriminant Δ of f is 0 as we have $\Delta = 4i_8 - 3i_4^2$, hence f has a twofold linear factor. So after a suitable transformation of coordinates, we have $f = x^2 z(x + z)(x + \lambda z)$ for some $\lambda \in \overline{k}^*$. Then we find that we have $i_4(f) = 2\lambda^2(\lambda^2 - \lambda + 1)$ and $i_{12}(f) = \lambda^6(4\lambda^6 + 3\lambda^5 + 8\lambda^4 + 4\lambda^3 + 8\lambda^2 + 3\lambda + 4)$. If we consider $i_4(f) \cdot \lambda^{-2}$ and $i_{12}(f) \cdot \lambda^{-6}$ as polynomials in terms of λ, we can compute their resultant and find that it is equal to 1. Thus it follows that there is no $\lambda \in \overline{k}^*$ such that $i_4(f) = i_{12}(f) = 0$.

Thus we find that f must have a threefold linear factor, hence is a null form. □

We can use this to prove the following theorem about reconstruction of binary quintics over these fields.

Theorem 4.7. *Let k be an algebraically closed field of characteristic 3. Let $B_5 \subset S^5(V)$ denote the space of binary quintic forms over k which do not posses a threefold linear factor. Then there is a bijection*

$$\begin{aligned} \mathrm{GL}_2(k)\backslash B_5 &\to \mathbb{P}^{(1,2,3)}(k), \\ [f] &\mapsto (i_4(f) : i_8(f) : i_{12}(f)). \end{aligned}$$

Moreover, if $(i_4 : i_8 : i_{12}) \in \mathbb{P}^{(1,2,3)}(k)$ *is a point defined over some field* l *such that* $l \subset k$*, then there exists a quintic* f *in the corresponding orbit with coefficients in* l*.*

Proof. First we note that the map is well-defined, as from Lemma 4.6 it follows that $i_4(f) = i_8(f) = i_{12}(f) = 0$ implies that f has a threefold linear factor, and i_4, i_8 and i_{12} are invariants whose respective weights scale by a $1 : 2 : 3$ ratio.

For the case $i_8 \neq 0$, surjectivity follows from the fact that the form $\overline{f}$ as defined in Equation (8) has the correct invariants. Now suppose that we have some point $(i_4 : 0 : i_{12}) \in \mathbb{P}^{(1,2,3)}(k)$. If $i_4 = 0$, the form $f = x^3z^2 + xz^4$ has the correct invariants. Else we can scale such that the point is of the form $(-1 : 0 : t)$ for some $t \in k$ and the form $f(x, z) = x^3z^2 + x^2z^3 + (t-1)z^5$ has the correct invariants. Hence the map is surjective.

To prove the map is injective as well, we can apply Lemma 3.3 for the case where $i_8 \neq 0$, as any two forms with the same invariants and non-zero i_8 are $\mathrm{GL}_2(k)$-equivalent. It remains to show this also holds for the case where i_8 vanishes.

Suppose we have a form f with $i_8(f) = 0$ and $i_4(f) \neq 0$ or $i_{12}(f) \neq 0$, then f has a double linear factor as its discriminant vanishes (we have $\Delta = i_8$ in characteristic 3). So, after a suitable linear transformation, we may assume that f is of the form $f(x, z) = x^3z^2 + a_3x^2z^3 + a_4xz^4 + a_5z^5$ for some $a_3, a_4, a_5 \in k$ where $i_4(f) = -a_3^2$ and $i_{12}(f) = a_3^6 - a_3^2a_4^2 + a_3^3a_5 + a_4^3$.

If we have $i_4(f) = 0$, then it follows that $a_3 = 0$ and $a_4 \neq 0$ as $i_{12}(f) \neq 0$. If we then choose $\lambda \in k$ that satisfies $\lambda^3 + a_4\lambda + a_5 = 0$ and apply the transformation $x \mapsto x + \lambda z$ to f, the resulting form is $x^3z^2 + a_4xz^4$, which is $\mathrm{GL}_2(k)$-equivalent to the form $x^3z^2 + xz^4$ found above.

Else we have $i_4(f) \neq 0$ and it follows that $a_3 \neq 0$. We can then apply the linear transformation $x \mapsto x + (a_4/a_3)z$ to f and obtain a form of the shape $g = x^3z^2 + a_3x^2z^3 + a_5z^5$ (i.e. $a_4 = 0$) with invariants $i_4(g) = -a_3^2$ and $i_{12}(g) = a_3^6 + a_3^3a_5$. Now let α be a 5th root of a_3 and let $\lambda = \alpha^2$ and $\mu = \alpha^{-3}$, then after applying the linear transformation $x \mapsto \lambda x$, $z \mapsto \lambda z$ we obtain a form of the shape $h = x^3z^2 + x^2z^3 + sz^5$ for some $s \in k$ with $i_4(h) = -1$ and $i_{12}(h) = 1 - s$. This is exactly the form as chosen above, hence it follows that the map is injective.

For a point defined $(i_4(f) : i_8(f) : i_{12}(f))$ over some field l, the quintic is defined over l in all of the constructions above, which proves the last part of the claim. □

4.2.3 Characteristic 5

Consider a field k of characteristic 5. As seen in 4.1.2, there is a subalgebra of the algebra of invariants $\mathcal{I}_5(k)$ generated by the invariants i_4, i_8, i_{12} and i_{18}. If we reduce α', β' and δ' (see Table 2) modulo 5, we find that they are

3 irreducible polynomials, so that we have 3 linear covariants of respective weights 5, 7 and 13. Hence we can use either the covariants $\alpha_5 = \overline{\alpha'}$ and $\beta_5 = \overline{\beta'}$ or the covariants α_5 and $\delta_5 = \overline{\delta'}$ as coordinates, with respective determinants $i_4^3 - i_{12}$ and $-2i_{18}$.

If we take α_5 and β_5 as coordinates and set $m = i_4^3 - i_{12}$, we find that for a quintic f with $m(f) \neq 0$ the corresponding transformed form is

$$m^5\overline{f} = A_0x^5 + A_1x^4z + A_2x^3z^2 + A_3x^2z^3 + A_4xz^4 + A_5z^5, \tag{9}$$

where

$$\begin{aligned}
A_0 &= -2i_{18}(i_4^2 + i_8)\\
A_1 &= 2i_4(i_4^3 - i_{12})(i_4^3 + 2i_4i_8 + i_{12})\\
A_2 &= -2i_{18}(i_4^3 - i_{12})\\
A_3 &= 2i_4^2(i_4^3 - i_{12})(i_4^3 + 2i_4i_8 + i_{12})\\
A_4 &= -2i_{18}i_4(i_4^3 - i_{12})\\
A_5 &= i_4^9 - 2i_4^7i_8 + i_4^5i_8^2 - i_4^4i_8i_{12} + i_4^3i_{12}^2 - i_{12}^3.
\end{aligned}$$

If we take α_5 and δ_5 as coordinates and set $n = -2i_{18}$, we find that for a quintic f with $n(f) \neq 0$ the corresponding transformed form is

$$n^5\overline{f} = A_0x^5 + A_1x^4z + A_2x^3z^2 + A_3x^2z^3 + A_4xz^4 + A_5z^5, \tag{10}$$

where

$$\begin{aligned}
A_0 &= -2i_{18}(i_4^2 + i_8)\\
A_1 &= i_{18}i_4(i_4^3 + 2i_4i_8 + i_{12})\\
A_2 &= i_{18}(-i_4^3 + i_{12})^2\\
A_3 &= 2i_{18}i_4^2(-i_4^3 + i_{12})(i_4^3 + 2i_4i_8 + i_{12})\\
A_4 &= -2i_{18}i_4(-i_4^7i_8 - i_4^5i_8^2 - i_4^4i_8i_{12} - 2i_4^3i_{12}^2 + i_{12}^3)\\
A_5 &= 2i_{18}(-i_4^3 + i_{12})(-2i_4^9 + 2i_4^7i_8 - 2i_4^5i_8^2 + 2i_4^6i_{12} - i_4^4i_8i_{12} + 2i_4^3i_{12}^2 + i_{12}^3)
\end{aligned}$$

So given a set of values for the invariants i_4, i_8 and i_{12}, such that either $i_4^3 - i_{12} \neq 0$ or $i_{18} \neq 0$, we can use this to reconstruct a binary quintic with the corresponding values for the invariants up to scaling. This leads to the following theorem.

Theorem 4.8. *Let k be an algebraically closed field of characteristic 5. Let $B_5 \subset S^5(V)$ denote the space of binary quintic forms over k which do not posses a threefold linear factor. Then there is a surjective map*

$$\begin{aligned}
\mathrm{GL}_2(k)\backslash B_5 &\to \mathbb{P}^{(1,2,3)}(k),\\
[f] &\mapsto (i_4(f) : i_8(f) : i_{12}(f)).
\end{aligned}$$

If $i_4^3 - i_{12} \neq 0$ or $i_{18} \neq 0$, there is a single orbit mapping to the point $(i_4 : i_8 : i_{12}) \in \mathbb{P}^{(1,2,3)}(k)$. If moreover $(i_4 : i_8 : i_{12}) \in \mathbb{P}^{(1,2,3)}(k)$ is a point defined over some field l such that $l \subset k$, then there exists a quintic f in the corresponding orbit with coefficients in l.

Proof. First we note that the map is well-defined, as from Lemma 4.6 it follows that $i_4(f) = i_8(f) = i_{12}(f) = 0$ implies that f has a threefold linear factor, and i_4, i_8 and i_{12} are invariants whose respective weights scale by a $1 : 2 : 3$ ratio.

For the case where $i_4^3 - i_{12} \neq 0$ or $i_{18} \neq 0$, surjectivity follows from the fact the form $\overline{f}$ as defined in Equation (9) or Equation (10) has the correct invariants. Moreover, if we have two forms mapping to the same point $(i_4 : i_8 : i_{12}) \in \mathbb{P}^{(1,2,3)}(k)$ with $i_4^3 - i_{12} \neq 0$ or $i_{18} \neq 0$, then they are $\mathrm{GL}_2(k)$-equivalent by Lemma 3.3.

Next we prove surjectivity for the case $i_4^3 - i_{12} = 0$ and $i_{18} = 0$. If $i_4 = 0$, it follows that $i_{12} = 0$, so that only i_8 does not vanish. One can check that the form $f = x(x^4 + z^4)$ has the correct invariants.

Else $i_4 \neq 0$, and we can scale such that $i_4 = 1$ and hence $i_{12} = 1$. Then Equation (6) implies that $i_{18}^2 = -(i_8 + 1)^2$ and as i_{18} vanishes, it follows that $i_8 = -1$. This corresponds to the weighted projective point $(1 : -1 : 1) \in \mathbb{P}^{(1,2,3)}(k)$, and the orbit of the form $f = xz(x^3 + z^3)$ maps to this point.

For a point defined $(i_4(f), i_8(f), i_{12}(f))$ over some field l, the quintic is defined over l by the construction above. □

Remark 4.9. *For the case where $i_4^3 - i_{12} = 0$ and $i_{18} = 0$, the forms in the proof above do have the right invariant values, but we cannot prove there are no other orbits mapping to these invariants. For uniqueness, one would have to compute the full ring of invariants $\mathcal{I}_5(k)$ (or a separating subset); see also Remark 4.3.*

References

[Cle1872] A. Clebsch. *Theorie der binären algebraischen Formen*. B.G. Teubner, 1872.

[DK2002] H. Derksen and G. Kemper. *Computational Invariant Theory*, volume 130 of *Encyclopaedia of Mathematical Sciences*. Springer-Verlag Berlin Heidelberg, 2002.

[dPW2018] A. du Plessis and C. T. C. Wall. The moduli space of binary quintics. *European Journal of Mathematics*, 4(1):423 – 436, March 2018.

[Gey1974] W. D. Geyer. Invarianten binärer formen. In H. Popp, editor, *Classification of algebraic varieties and compact complex manifolds*, volume 412 of *Lecture Notes in Mathematics*, pages 36 – 69. Springer, 1974.

[GY1903] J. H. Grace and A. Young. *The algebra of invariants*. Cambridge University Press, 1903.

[Hil1993] D. Hilbert. *Theory of algebraic invariants*. Cambridge University Press, 1993. Course notes of a German course in 1897, translated by R. C. Laubenbacher and edited by B. Sturmfels.

[Igu1960] J.-I. Igusa. Arithmetic variety of moduli for genus two. *Annals of Mathematics*, 72(3):612–649, 1960.

[LR2012] R. Lercier and C. Ritzenthaler. Hyperelliptic curves and their invariants: Geometric, arithmetic and algorithmic aspects. *Journal of Algebra*, 372(Supplement C):595 – 636, December 2012.

[Mcl2008] C. Mclarty. Theology and its discontents: David Hilbert's foundation myth for modern mathematics, April 2008. https://webusers.imj-prg.fr/~michael.harris/theology.pdf.

[Mes1991] J.-F. Mestre. Construction de courbes de genre 2 à partir de leurs modules. In T. Mora and C. Traverso, editors, *Effective methods in algebraic geometry*, pages 313 – 334. Springer, 1991.

[Nag1963] M. Nagata. Invariants of group in an affine ring. *J. Math. Kyoto Univ.*, 3(3):369–378, 1963.

[Som2019] A. Somoza Henares. *Inverse Jacobian and related topics for certain superelliptic curves*. PhD thesis, Universiteit Leiden & Universitat Politècnica de Catalunya, March 2019.

[Sage] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 8.4)*, October 2018. https://www.sagemath.org.

[Rov2017] F. Ulpat Rovetta. A strategy and a new operator to generate covariants in small characteristic. *arXiv e-prints*, January 2017, 1701.09165.

[Yal1966] P. B. Yale. Automorphisms of the complex numbers. *Mathematics Magazine*, 39(3):135–141, 1966.