15

Binary Forms

We want to finish this book going backwards in history. After having discussed many topics mostly belonging to 20^{th} century mathematics, we go back to where they all began, the old invariant theory of the 19^{th} century in its most complete achievement: the theory of binary forms. We show a few of the many computational ideas which were developed at that time.

For a classical exposition see the book by Grace and Young [GY].

1 Covariants

1.1 Covariants

The theory of binary forms studies the invariants of forms in two variables.

Recall that the space of binary forms of degree m is the space:[142]

$$S_m := \left\{ \sum_{i=0}^{m} a_i \binom{m}{i} x^{m-i} y^i \mid a_i \in \mathbb{C} \right\}. \tag{1.1.1}$$

Of course one can also study binary forms over more general coefficient rings.

We have seen that the spaces S_m are irreducible representations of $SL(2, \mathbb{C})$ and in fact exhaust the list of these representations. The observation that S_m has a non-degenerate $SL(2, \mathbb{C})$ invariant form (Chapter 5, §3.7) implies that S_m and S_m^* are isomorphic representations.

The algebra of invariants of binary forms of degree m is the ring of polynomials in the coordinates $(a_0, a_1, \ldots, a_m)$ which are invariant under the action of $SL(2, \mathbb{C})$. Many papers on this subject appeared in the 19^{th} century, but then the theory disappeared from the mathematical literature, to be discovered again in the last 30 years.

Let us establish some notation. Denote by $S(S_m)$, $P(S_m) = \mathbb{C}[a_0, a_1, \ldots, a_m]$, respectively, the symmetric algebra and the polynomials on the space S_m. These two

[142] The normalization of the coefficients is for convenience.

algebras are both representations of $SL(2,\mathbb{C})$ and in fact they are isomorphic as representations due to the observation that S_m has a nondegenerate $SL(2,\mathbb{C})$ invariant form. Since $SL(2,\mathbb{C})$ is the only group in this chapter, we will write for short $SL(2,\mathbb{C}) = S(2)$.

There are several ways to approach the theory, but almost always they pass through the study of a more general problem: the study of *covariants.*

Definition. On the space of forms of degree m, a covariant of degree k and order p is a polynomial map $F : S_m \to S_p$, homogeneous of degree k and $S(2)$-equivariant.

Of course an invariant is just a covariant of order 0.

Remark. The first remark to be made is the obvious one. The identity map $f \to f$ of S_m is a covariant of degree 1 and order m. The form f is a covariant (of itself).

A polynomial map $F : S_m \to S_p$, homogeneous of degree k, is the composition of a linear map $f : S^k[S_m] \to S_p$ with $a \mapsto a^k$, where $S^k[S_m]$ is the k-th symmetric power of S_m. Let $M_p(k, m)$ denote the isotypic component of $S^k[S_m]$ of type S_p. We have that $M_p(k,m) = S_p \otimes V_p(k,m)$, where $\dim V_p(k,m)$ is the multiplicity with which S_p appears in $S^k[S_m]$.

Proposition 1. *The space of covariants of degree k and order p is the dual of $V_p(k,m)$.*

Proof. Since $\hom_{S(2)}(S_p, S_p) = \mathbb{C}$, the explicit identification is the following:

$$\begin{aligned}\hom_{S(2)}(S^k[S_m], S_p) &= \hom_{S(2)}(S_p \otimes V_p(k,m), S_p)\\ &= \hom_{S(2)}(S_p, S_p) \otimes V_p(k,m)^*. \qquad \square\end{aligned}$$

This proposition of course implicitly says that knowing covariants is equivalent to knowing the decomposition of $S(S_m)$ into isotypic components.

There is a different way of understanding covariants which is important. Consider the space $V = \mathbb{C}^2$ on which $S_m = S^m[V^*]$ is identified with the space of homogeneous polynomials of degree m. Although by duality V is isomorphic to S_1, it is important to distinguish the two spaces. On V we have the two coordinates x, y. Consider the $S(2)$ invariant polynomials on the space $S_m \oplus V$. Call the variables $(a_0, a_1, \dots, a_m, x, y)$. Any polynomial invariant $f(a_0, a_1, \dots, a_m, x, y)$ decomposes into the sum of the bihomogeneous parts with respect separately to S_m and V. These components are invariant.

Proposition 2. *The space of covariants of degree k and order p on S_m can be identified with the space of invariants on $S_m \oplus V$ of bidegree k, p.*

Proof. If $F : S_m \to S_p$ is a covariant and $a \in S_m$, $v \in V$, we can evaluate $F(a)(v)$, and this is clearly an invariant function of a, v. If $\lambda, \mu \in \mathbb{C}$, we have

$$F(\lambda a)(\mu v) = \lambda^k F(\mu v) = \lambda^k \mu^p F(v).$$

Conversely, if $F(a_0, a_1, \dots, a_m, x, y)$ is a bihomogeneous invariant of bidegree k, p, we have that for fixed $a = (a_0, a_1, \dots, a_m)$, the function $F(a_0, a_1, \dots, a_m, x, y)$ is a homogeneous form $f_a \in S_p$. The map $a \to f_a$ is equivariant and of degree k. $\square$

In more explicit terms we write an invariant of bidegree k, p as

$$f(a_0, a_1, \dots, a_m, x, y) = \sum_{i=0}^{p} f_i(a_0, a_1, \dots, a_m) x^{p-i} y^i$$

which exhibits its nature as a covariant.

1.2 Transvectants

Of course covariants may be composed and defined also for several binary forms. The main construction between forms and covariants is *transvection*.[143]

Transvection is an interpretation of the Clebsch–Gordan formula, which in representation theoretic language is

$$S_p \otimes S_q = \bigoplus_{i=0}^{\min(p,q)} S_{p+q-2i}. \tag{1.2.1}$$

Definition. Given $f \in S_p$, $g \in S_q$, the i^{th} transvection $(f, g)_i$ of f, g is the projection of $f \otimes g$ to S_{p+q-2i}.

It is interesting and useful to see the transvection explicitly in the case of *decomposable* forms. Since $S_m = S_m(S_1)$ we follow the usual procedure of tensor algebra to make explicit a multilinear function on decomposable tensors.

Let us use the classical notation in which several forms are thought of as depending on different sets of variables, denoted $x, y, z, \dots$. So we change the notation slightly.

Given a linear form $a = a_x := a_0 x_1 + a_1 x_2$ the form

$$a_x^m = \sum_{i=0}^{m} a_0^{m-i} a_1^i \binom{m}{i} x_1^{m-i} x_2^i$$

is a typically decomposable form. If $b_y = b_0 y_1 + b_1 y_2$ is another linear form let us define (a, b) by

$$(a, b) := \det \begin{vmatrix} a_0 & a_1 \\ b_0 & b_1 \end{vmatrix} = a_0 b_1 - a_1 b_0.$$

Proposition. *We have for the i^{th} transvection:*

$$(a_x^p, b_y^q)_i = (a, b)^i a_x^{p-i} b_x^{q-i}. \tag{1.2.2}$$

Proof. One can make explicit the computations of Chapter 3, §3.1.7, or argue as follows.

Consider the polynomial map:

$$T_i : (a_x, b_y) \to (a, b)^i a_x^{p-i} b_x^{q-i} \in S_{p+q-2i}, \tag{1.2.3}$$

T_i is clearly homogeneous of degree p in a_x and of degree q in b_y, therefore it factors as

$$(a_x, b_y) \mapsto a_x^p \otimes b_y^q \in S_p \otimes S_q \xrightarrow{t_i} S_{p+q-2i}.$$

[143] *Übershiebung* in German.

It is clear that T_i is $S(2)$-equivariant, hence also $S_p \otimes S_q \xrightarrow{t_i} S_{p+q-2i}$ is a linear equivariant map. At this point there is only one subtlety to discuss. While the projection to the isotypic component of $S_p \otimes S_q$ of type S_{p+q-2i} is uniquely determined, the explicit isomorphism of this component with S_{p+q-2i} is determined up to a scalar, so we can in fact *define* the transvection so that it is normalized by the formula 1.2.2. □

Given two covariants $F : S_m \to S_p$, $G : S_m \to S_q$ we can then form their transvection $(F, G)_i : S_m \to S_{p+q-2i}$. As in the general theory we may want to polarize a covariant $F : S_m \to S_p$ of degree k by introducing k variables in S_m. We obtain then a multilinear covariant

$$\overline{F} : S_m \otimes S_m \otimes \cdots \otimes S_m \to S_p.$$

Iterating the decomposition 1.2.1 as normalized by 1.2.2 we obtain a decomposition:

$$S_m^{\otimes k} = \bigoplus_{i_1, i_2, \ldots, i_{k-1}} S_{km-2(i_1+i_2+\cdots+i_{k-1})},$$
$$i_j \leq \min(m, jm - 2(i_1 + i_2 + \cdots + i_{j-1})).$$

This is an explicit way in which $S_m^{\otimes k}$ can be decomposed into irreducible summands.

On an element $f_1 \otimes f_2 \otimes \cdots \otimes f_k$, $f_i \in S_m$, the projection onto $S_{km-2(i_1+i_2+\cdots+i_{k-1})}$ is the iteration of transvections:

$$(((\ldots((f_1, f_2)_{i_1}, f_3)_{i_2}, \ldots, f_k)_{i_k}.$$

For instance, quadratic covariants of a given form f are only the transvections $(f, f)_i$.

Theorem. *Any covariant of f is a linear combination of covariants obtained from f by performing a sequence of transvections.*

1.3 Source

Given a covariant, thought of as an invariant

$$f(a_0, \ldots, a_m, x, y) = \sum_{i=0}^{p} f_i(a_0, \ldots, a_m) x^{p-i} y^i,$$

let us compute it for the vector of coordinates $x = 1, y = 0$, getting

$$f(a_0, \ldots, a_m, 1, 0) = f_0(a_0, a_1, \ldots, a_m).$$

Definition. The value $f_0(a_0, a_1, \ldots, a_m)$ is called the source[144] of the covariant.

Example. For the identity covariant f the source is a_0.

[144] *Quelle* in German.

The main point is:

Theorem 1. *The source of a covariant is invariant under the subgroup* $U^+ := \left\{\begin{vmatrix} 1 & u \\ 0 & 1 \end{vmatrix}\right\}$. *Every* U^+ *invariant function* $f_0(a_0, a_1, \dots, a_m)$ *is the source of a covariant. The map*

$$Q : f(a_0, \dots, a_m, x, y) \to f(a_0, \dots, a_m, 1, 0) = f_0(a_0, a_1, \dots, a_m)$$

is an isomorphism between covariants and U^+ *invariants of* S_m.

Proof. Given a covariant $f(a, v)$, since $(1, 0)$ is a vector invariant under U^+ and f is invariant under $SL(2)$, clearly $f(a, (1, 0))$ is U^+-invariant. For the converse we need an important geometric remark. Let $\mathcal{A} := \{(a, v) \in S_m \times V \mid v \neq 0\}$. $\mathcal{A}$ is an open set and its complement is S_m, so it has codimension 2 in the ambient space. Let $S'_m := \{(a, (1, 0)), a \in S_m\} \subset S_m \oplus V$. Given any element $(a, v) \in \mathcal{A}$ there is an element $g \in SL(2)$ with $gv = (1, 0)$. In other words $SL(2)S'_m = \mathcal{A}$. It follows that any $SL(2)$ invariant function is determined by the values that it takes once restricted to S'_m, and this is exactly the map Q. It remains to prove that, given a U^+ invariant function on S'_m, it extends to an $SL(2)$-invariant function on $S_m \times V$. In fact it is enough to show that it extends to an algebraic function on $\mathcal{A}$, since then it extends everywhere due to the codimension condition. The argument is this: given $\overline{f}$ a U^+-invariant we want to define an extension of f on $\mathcal{A}$. Take a vector (a, v) and a $g \in SL(2)$ with $gv = (1, 0)$ and define $f(a, v) := \overline{f}(ga, (1, 0))$. We need to show that this is well defined. This follows from the U^+-invariance and the fact that it is a regular algebraic function, which is a standard fact of algebraic geometry due to the smoothness of $\mathcal{A}$.

In more concrete terms, given (x, y) if $x \neq 0$ (resp. $y \neq 0$) we construct

$$\begin{vmatrix} x \\ y \end{vmatrix} = \begin{vmatrix} x & 1 \\ y & \frac{y+1}{x} \end{vmatrix} \begin{vmatrix} 1 \\ 0 \end{vmatrix}, \qquad \begin{vmatrix} x \\ y \end{vmatrix} = \begin{vmatrix} x & \frac{x-1}{y} \\ y & 1 \end{vmatrix} \begin{vmatrix} 1 \\ 0 \end{vmatrix}.$$

When we use these two matrices as the g to build the function $f(a, v) := \overline{f}(ga, (1, 0))$ we see that it has an expression as a polynomial in $a_0, \dots, a_m, x, y$ with denominator either a power of x or of y, and hence this denominator can be eliminated. $\square$

Remark. In the classical literature an invariant under the subgroup U^+ is also called a *semi-invariant.*

We need to understand directly from the nature of the semi-invariant what type of covariant it is. For this we introduce the notion of weight. At the beginning the notion is formal, but in fact we will see that it is a weight in the sense of characters for the multiplicative group. By definition we give weight i to the variable a_i and extend (by summing the weights) the notion to the weight of a monomial. A polynomial is usually called *isobaric* if it is a sum of monomials of the same weight. In this case we can talk of the weight of the polynomial.

Theorem 2. *The source of a covariant of degree k and order p, of forms in S_m, is a homogeneous polynomial of degree k which is isobaric of weight $\frac{mk-p}{2}$. In particular an $SL(2)$-invariant on S_m, is a semi-invariant of degree k and weight $\frac{mk}{2}$.*

Proof. Consider the torus $D_t := \begin{vmatrix} t^{-1} & 0 \\ 0 & t \end{vmatrix} \subset SL(2)$. It acts on the space V transforming $x \mapsto t^{-1}x,\ y \mapsto ty$. The action on the forms is

$$(D_t f)(x, y) = f(tx, t^{-1}y), \sum_{i=0}^{m} a_i \binom{m}{i} (tx)^{m-i}(t^{-1}y)^i = \sum_{i=0}^{m} a_i \binom{m}{i} t^{m-2i} x^{m-i} y^i.$$

In other words D_t transforms $a_i \to t^{m-2i}a_i$. A covariant, of degree k and order p, must be also an invariant function of this transformation on $S_m \oplus V$ or

$$f(t^m a_0, \dots, t^{m-2i}a_i, \dots, t^{-m}a_m, t^{-1}x, ty) = f(a_0, \dots, a_m, x, y).$$

For the source we get

$$f_0(t^m a_0, \dots, t^{m-2i}a_i, \dots, t^{-m}a_m)(t^{-1}x)^p = f_0(a_0, \dots, a_m)x^p.$$

A monomial in f_0 of weight w is multiplied by t^{mk-2w}; hence we deduce that for every monomial $mk - 2w - p = 0$, as required. □

In particular notice:[145]

Corollary. *The $SL(2)$-invariants of binary forms of degree k are the semi-invariants of degree k and of weight $\frac{mk}{2}$.*

If $B := \left\{ \begin{vmatrix} t^{-1} & u \\ 0 & t \end{vmatrix} \right\}$, the B-invariants coincide with the $SL(2)$-invariants.

Proof. The first assertion is a special case of the previous theorem. The second follows from the proof: a semi-invariant of degree k is invariant under B if and only if its weight w satisfies $mk - 2w = 0$, and then $p = 0$. □

2 Computational Algorithms

2.1 Recursive Computation

The theory of semi-invariants allows one to develop a direct computational method which works very efficiently to compute covariants of forms of low degree, and then its efficiency breaks down! Denote by A_m the ring of polynomial semi-invariants of binary forms of degree m.

First, a little remark. On binary forms the action of U^+ fixes y and transforms $x \mapsto x + ty$, therefore it commutes with $\frac{\partial}{\partial x}$. Moreover the 1-parameter group U^+ is

[145] The reader experienced in algebraic geometry may see that the geometric reason is in the fact that $SL(2)/B = \mathbb{P}^1$ is compact.

the exponential of the element $y\frac{\partial}{\partial x}$. This element acts as a unique nilpotent Jordan block of size $m+1$ on the space S_m. Thus the theory of semi-invariants is the theory of invariants under the exponential of this unique block.

The previous remark implies that the maps

$$i_m : S_m \to S_{m+1},\ i_m(f(x,y)) := f(x,y)y,$$

$$p_{m+1} : S_{m+1} \to S_m,\ p_{m+1}(f(x,y)) := \frac{\partial}{\partial x} f(x,y)$$

are U^+-equivariant. In particular they induce two maps $i_m^* : A_{m+1} \to A_m,\ p_{m+1}^* : A_m \to A_{m+1}$. We have $p_{m+1} i_m = i_{m-1} p_m$.

We will use in particular $p^* := p_{m+1}^*$ to build A_{m+1} starting from A_m.

If we take the basis $u_{i,m} := \frac{1}{i!} x^i y^{m-i}$ we have

$$p(u_{i,m})) = u_{i-1,m-1},\ 1 \le i \le m,\ p(u_{0,m})) = 0.$$

Therefore it is convenient to write the forms as:[146]

$$\sum_{i=0}^{m} a_i \frac{1}{(m-i)!} x^{m-i} y^i. \tag{2.1.1}$$

so that $y\frac{\partial}{\partial x} \sum_{i=0}^m a_i \frac{1}{(m-i)!} x^{m-i} y^i = \sum_{i=0}^{m-1} a_i \frac{1}{(m-i-1)!} x^{m-i-1} y^{i+1}$. Passing to coordinates, the transpose transformation maps $a_i \mapsto a_{i-1}$. Thus the differential operator which generates the induced group of linear transformations on the polynomial ring $F[a_0, \dots, a_m]$ is

$$-\sum_{i=1}^{m} a_{i-1} \frac{\partial}{\partial a_i}.$$

Proposition. *A polynomial $f(a_0, \dots, a_m)$ is a semi-invariant if and only if it satisfies the differential equation:*

$$\sum_{i=1}^{m} a_{i-1} \frac{\partial}{\partial a_i} f(a_0, \dots, a_m) = 0. \tag{2.1.2}$$

The operator $\sum_{i=1}^m a_{i-1} \frac{\partial}{\partial a_i}$ maps polynomials of degree k and weight p into polynomials of degree k and weight $p-1$.

Let us take a form $\sum_{i=0}^m a_i \frac{1}{(m-i)!} x^{m-i} y^i$ with $a_0 \neq 0$. Under the transformation $x \to x - \frac{a_1}{a_0} y,\ y \to y$, it is transformed into a form with $a_1 = 0$. More formally, let S_m^0 be the set of forms of degree m with $a_0 \neq 0$ and let S_m' be the set of forms of degree m with $a_0 \neq 0,\ a_1 = 0$. The previous remark shows that, acting with U^+, we identify $S_m^0 = U^+ \times S_m'$. Thus we have an identification of the U^+-invariant functions on S_m^0 with the functions on S_m'. The functions on S_m' are the polynomials in their

[146] In fact the algorithm could be easily done in all characteristics, in which case it is important to choose the correct basis. The reader may do some exercises and verify that covariants change when the characteristic is small.

coefficients with a_0 inverted. Let us denote by b_i the U^+-invariant function on S_m^0 which corresponds to the i^{th} coefficient, $i = 2, \dots, m$, of forms in S'_m. Calculating explicitly the functions b_i we have

$$a_0^m \sum_{i=0}^m a_i \frac{1}{(m-i)!}\left(x - \frac{a_1}{a_0}y\right)^{m-i} y^i = \sum_{i=0}^m a_0^i a_i \frac{1}{(m-i)!}(a_0x - a_1y)^{m-i}y^i$$

$$= \sum_{i=0}^m a_i \sum_{j=0}^{m-i} a_0^{m-j}(-a_1)^j \frac{1}{j!}\frac{1}{(m-i-j)!}x^{m-i-j}y^{i+j}$$

$$= \sum_{k=0}^m \left[\sum_{j=0}^k a_{k-j}a_0^{m-j}(-a_1)^j \frac{1}{j!}\right]\frac{1}{(m-k)!}x^{m-k}y^k \implies$$

$$b_k = a_0^{-m}\left[\sum_{j=0}^k a_{k-j}a_0^{m-j}(-a_1)^j \frac{1}{j!}\right].$$

Let

$$(1-k)c_k := (-1)^k k! a_0^{k-1} b_k = \sum_{j=0}^k (-1)^{k+j}\frac{k!}{j!}a_0^{k-j-1}a_{k-j}a_1^j$$

$$= (1-k)a_1^k + \sum_{s=2}^k \frac{(-1)^s k!}{(k-s)!}a_0^{s-1}a_s a_1^{k-s}.$$

We have thus proved:

Theorem. *The ring* $A_m[a_0^{-1}] = F[c_2, \dots, c_m][a_0, a_0^{-1}]$.

Let us make explicit some of these elements:

$$c_2 = a_1^2 - 2a_0a_2$$

$$c_3 = a_1^3 - 3a_0a_2a_1 + 3a_0^2a_3$$

$$c_4 = a_1^4 - 4a_0a_2a_1^2 + 8a_0^2a_3a_1 - 8a_0^3a_4$$

$$c_5 = a_1^5 - 5a_0a_2a_1^3 + 15a_0^2a_3a_1^2 - 30a_0^3a_4a_1 + 30a_0^4a_5$$

$$c_6 = a_1^6 - 6a_0a_2a_1^4 + 24a_0^2a_3a_1^3 - 72a_0^3a_4a_1^2 + 144a_0^4a_5a_1 - 144a_0^5a_6.$$

We have that c_i is a covariant of degree i and weight i.

If we want to understand covariants from these formulas it is necessary to compute

$$(2.1.3) \qquad A_m = F[c_2, \dots, c_m][a_0, a_0^{-1}] \cap F[a_0, \dots, a_m].$$

For each polynomial $F(c_2, \dots, c_m)$ we need to consider its order of vanishing for $a_0 = 0$. Write $F(c_2, \dots, c_m) = a_0^k G(a_0, a_1, a_2, \dots, a_m)$ with $G(0, a_1, a_2, \dots, a_m) \neq 0$. Then we may add $G(a_0, a_1, a_2, \dots, a_m)$ to A_m.

Remark. We have that $A_m \subset A_{m+1}$. Moreover the elements c_i are *independent* of m (the ones which exist).

We may now make a further reduction:

Exercise. If a covariant $G(a_0, a_1, a_2, \dots, a_m)$ satisfies $G(0, a_1, a_2, \dots, a_m) \neq 0$, then we also have $G(0, a_1, 0, \dots, a_m) \neq 0$. It follows that if we define $d_2 := c_2(a_0, a_1, 0, a_3, \dots, a_m)$ and $\overline{A}_m = F[d_2, \dots, d_m][a_0, a_0^{-1}] \cap F[a_0, a_1, a_3, \dots, a_m]$, then the natural map $A_m \to \overline{A}_m$ is an isomorphism.

Let us explain how we proceed. Suppose we have already constructed $A_m = F[t_1, t_2, \dots, t_k]$ and want to compute A_{m+1}. We add c_{m+1} to A_m and then want to find the elements in $F[t_1, t_2, \dots, t_k, c_{m+1}]$ which are divisible by a_0 or a power of it.

For this we evaluate the elements $t_1, t_2, \dots, t_k, c_{m+1}$ for $a_0 = 0$. For these evaluated elements consider their ideal of relations. Each element in this ideal lifts to a polynomial $h[t_1, t_2, \dots, t_k, c_{m+1}]$ which is divisible by a_0. We then start determining a set of generators for the ideal lifting to polynomials $h_i[t_1, t_2, \dots, t_k, c_{m+1}] = a_0^k g_i[a_0, a_1, \dots, a_{m+1}]$ where $g_i[0, a_1, \dots, a_{m+1}] \neq 0$. The elements $g_i[a_0, a_1, \dots, a_{m+1}] \in A_{m+1}$ and we add them. In this way we may not have added all the elements coming from the ideal, but we have that:

Lemma. *Let $a_0 = s_0, s_1, \dots, s_k \in F[a_0, a_1, \dots, a_m]$, and denote by $\overline{s}_i := s_i(0, a_1, \dots, a_m)$. Assume we have a basis $h_i[x_1, x_2, \dots, x_k]$ of the ideal J of relations between the elements $\overline{s}_1, \dots, \overline{s}_k$. Then write*

$$h_i[s_1, s_2, \dots, s_k] = a_0^{k_i} g_i[a_0, a_1, \dots, a_{m+1}],$$

with $g_i[0, a_1, \dots, a_m] \neq 0$. Assume furthermore that for every i we have $g_i[a_0, a_1, \dots, a_{m+1}] \in F[s_0, s_1, \dots, s_k]$.

Then for every $h[x_1, x_2, \dots, x_k] \in J$, such that

$$h[s_0, s_1, s_2, \dots, s_k] = a_0^k g[a_0, a_1, \dots, a_m],$$

we have $g[a_0, a_1, \dots, a_m] \in F[s_0, s_1, \dots, s_k]$.

Proof. Let us work by induction on the order of vanishing k. If $k = 0$, there is nothing to prove, otherwise $h[x_1, x_2, \dots, x_k] \in J$, and let

$$h[x_1, x_2, \dots, x_k] = \sum_i t_i[x_1, x_2, \dots, x_k] h_i[x_1, x_2, \dots, x_k].$$

We substitute for the x_i the s_i, and pull out the powers of a_0 and get

$$a_0^k g[a_0, a_1, \dots, a_m] = \sum_i t_i[s_1, \dots, s_k] a_0^{k_i} g_i[a_0, a_1, \dots, a_m].$$

All the k_i are positive and of course $k \geq \min k_i := h > 0$. We cancel h and

$$a_0^{k-h} g[a_0, a_1, \dots, a_m] = \sum_i t_i[s_1, \dots, s_k] a_0^{k_i - h} g_i[a_0, a_1, \dots, a_m].$$

By hypothesis $a_0, g_i[a_0, a_1, \dots, a_m] \in F[s_0, s_1, \dots, s_k]$, hence we finish by induction. □

The previous lemma gives an algorithm to compute A_m. At each step we have determined some ring $F[s_0, s_1, \dots, s_k]$ and we add to this ring all the elements g_i obtained from a basis of the ideal J. When no new elements are found the algorithm stops.

Of course it is not a priori clear that the algorithm will stop; in fact this is equivalent to the classical theorem that covariants are a finitely generated algebra.

On the other hand, if one keeps track of the steps in the algorithm, one has also a presentation for the covariant algebra by generators, relations and the relations among the relations, i.e., the syzygies.

We can perform this explicitly for $m \leq 6$. For $m \leq 4$ we easily define, following the previous algorithm, covariants A, B, C by

$$(2.1.4) \qquad 3Aa_0^2 = c_2^3 - c_3^2, \quad c_4 - c_2^2 = 8Ba_0^2, \quad A - 2Bc_2 = a_0 C.$$

Since by standard theory A_m is a ring of dimension m we get that

$$(2.1.5) \qquad A_2 = F[a_0, c_2], \ A_3 = F[a_0, c_2, c_3, A], \ A_4 = F[a_0, c_2, c_3, B, C],$$

where in A_2 the elements a_0, c_2 are algebraically independent, while for A_3, A_4, we have one more generator than the dimension and the corresponding equations 2.1.4. One may continue by hand for 5,6 but the computations become more complicated and we leave them out.

By weight considerations and Corollary 1.3, one can identify, inside the covariants, the corresponding rings of invariants.

2.2 Symbolic Method

The symbolic method is the one mostly used in classical computations. It is again based on polarization. Let us denote by V the space of linear binary forms and by $S^m(V)$ their symmetric powers, the binary forms of degree m.

One chooses the coefficients so that a form is written as $A := \sum_{i=0}^m a_i \binom{m}{i} x^{m-i} y^i$. This is convenient since, when the form is a power of a linear form $b_1 x + b_2 y$, we obtain $a_i = b_1^{m-i} b_2^i$.

Let $h(A) = h(a_0, \dots, a_m)$ be a polynomial invariant, homogeneous of degree k, for binary forms of degree m. Polarizing it we deduce a multilinear invariant of k forms $h(A_1, \dots, A_k)$. Evaluating this invariant for $A_i := b_i^m$ with b_i a linear form, we obtain an invariant of the linear forms $b_1, \dots, b_k$ which is symmetric in the b_i and homogeneous of degree m in each b_i. Now one can use the FFT for $SL(2)$ proved in Chapter 11, §1.2 (which in this special case could be proved directly), and argue that any such invariant is a polynomial in the determinants $[b_i, b_j]$. Conversely any invariant of the linear forms $b_1, \dots, b_k$ which is homogeneous of degree m in each $b_i \in V$, factors uniquely through a multilinear invariant on the symmetric powers $S^m(V)$. Under restitution one obtains a homogeneous polynomial invariant of binary forms of degree k. Thus:

Theorem 1. *The space of polynomial invariants, homogeneous of degree k, for binary forms of degree m is linearly isomorphic to the space of invariants of k linear forms, homogeneous of degree m in each variable and symmetric in the k forms.*

In practice this method gives a computational recipe to produce a complete list of linearly generating invariants in each degree. One writes a basis of invariants of k linear forms, homogeneous of degree m, choosing products of elements $[b_i, b_j]$ with the only constraint that each index $i = 1, \dots, k$ appears exactly m times. Any such product is a *symbolic invariant.*

Next, one develops the polynomial using the formula

$$[b_i, b_j] = b_{i1}b_{j2} - b_{j1}b_{i2}$$

and looks at any given monomial which will necessarily, by the homogeneity condition, be of the form

$$\lambda_{h_1,h_2,\dots,h_k} b_{11}^{m-h_1} b_{12}^{h_1} b_{21}^{m-h_2} b_{22}^{h_2} \cdots b_{k1}^{m-h_k} b_{k2}^{h_k}.$$

Under the identifications made the invariant is obtained by the substitutions

$$\lambda_{h_1,h_2,\dots,h_k} b_{11}^{m-h_1} b_{12}^{h_1} b_{21}^{m-h_2} b_{22}^{h_2} \cdots b_{k1}^{m-h_k} b_{k2}^{h_k} \mapsto \lambda_{h_1,h_2,\dots,h_k} a_{h_1} a_{h_2} \cdots a_{h_k}.$$

In the previous discussion we have not assumed that the invariant of linear forms is necessarily symmetric. Let us then see an example. Suppose we want to find invariants of degree 2 for forms of degree m. In this case we prefer to write a, b instead of b_1, b_2 and have only one possible symbolic invariant, i.e., $[a, b]^m$. This is symmetric if and only if m is even; thus we have the existence of a quadratic invariant only for forms of even degree. For these forms we already know the existence of an $SL(2)$-invariant quadratic form which, up to normalization is the invariant of Chapter 5, §3.7.

In a similar way one may describe symbolically the invariants of several binary forms, of possibly different degrees.

Covariants can also be treated by the symbolic method. We can use the fact that according to Chapter 5, §3.7 there is a nondegenerate $SL(2)$-invariant bilinear form $\langle x, y\rangle$ on each space $S^p(V)$. Thus if $F : S^m(V) \to S^p(V)$ is a covariant of degree k and we polarize it to $\overline{F}(A_1, \dots, A_k)$, we obtain an invariant of $A_1, \dots, A_k \in S^m(V)$, $B \in S^p(V)$ by the formula $\langle F(A_1, \dots, A_k), B\rangle$. Next, we substitute as before A_i with b_i^m and B with c^p and get a linear combination of products of either (b_i, b_j) or (b_i, c). Conversely, given such a product, we can associate to it a covariant by taking the product of all the terms (b_i, b_j) in the monomial times the product of the b_j's which are paired with c. The previous discussion implies that all covariants will be obtained this way.

There are several difficulties involved with the symbolic method. One is the difficulty of taking care in a combinatorial way of the symmetry. In fact in Chapter 13, §2.3 we have shown that for invariants of several linear forms $b_1, \dots, b_k$ we have a theory of standard rectangular tableaux with rows of length 2 and filled with the numbers $1, 2, \dots, k$. The constraint that they be homogeneous of degree m in each variable means that each index i appears m times, but the symmetry condition is unclear in the combinatorial description and does not lead to another combinatorial constraint.

The second difficulty arises when one wants to build the invariant ring by generators and relations. It is not at all clear how to determine when a symbolic invariant can be expressed as a polynomial of lower degree symbolic invariants. This point was settled by Gordan in a very involved argument, which was later essentially forgotten once the more general theorems of Hilbert on the finite generation of invariants were proved.

Remark. A different proof of the symbolic method could be gotten directly using transvectants as in §2.

There is a second form in which the symbolic method appears and it is based on the following fact (we work over $\mathbb{C}$).

Let us consider the space of m-tuples of linear forms $(a_1, a_2, \dots, a_m)$ and the map to $S^m(V)$ given by

$$\phi : (a_1, a_2, \dots, a_m) \to \prod_{i=1}^{m} a_i .$$

The map ϕ is invariant under the action of the group N generated by the permutations S_m of the linear forms, and the rescaling of the forms

$$(a_1, a_2, \dots, a_m) \mapsto (\lambda_1 a_1, \lambda_2 a_2, \dots, \lambda_m a_m), \quad \prod_{i=1}^{m} \lambda_i = 1.$$

$N = S_m \ltimes T$ is the semidirect product of S_m with the torus

$$T := \{(\lambda_1, \lambda_2, \dots, \lambda_m)\}, \ \prod_{i=1}^{m} \lambda_i = 1.$$

The property of unique factorization implies that two m-tuples of linear forms map under ϕ to the same form of degree m if and only if they are in the same orbit under N. We claim then that:

Proposition. *The ring of invariants of the action of N on the space V^m of m-tuples $a_1, \dots, a_m$ of linear forms is the ring of polynomials in the coordinates of $S^m(V)$.*

Proof. Consider the quotient variety $V^m//N$. The map ϕ factors through the quotient as $\phi : V^m \xrightarrow{\pi} V^m//N \xrightarrow{\overline{\phi}} S^m(V)$. By the fact that $V^m//N$ parameterizes closed orbits of N, it follows that $\overline{\phi}$ is bijective. Hence, by ZMT, we have that $\overline{\phi}$ is an isomorphism. □

Now when we look at the invariants of $SL(2)$ on forms in $S^m(V)$ we have:

Theorem 2. *The invariants under $SL(2)$ on $S^m(V)$ coincide with the invariants under $N \times SL(2)$ acting on V^m.*

In particular the invariants under $SL(2)$ on $S^m(V)$ coincide with the invariants under N acting on the $SL(2)$-invariants of V^m.

We know that the $SL(2)$-invariants of V^m are described by standard rectangular tableaux with 2 columns and with entries $1, 2, \dots, m$. It is clear by the definitions that such a tableau U transforms under a torus element $(\lambda_1, \lambda_2, \dots, \lambda_m)$ as

$$\lambda_1^{h_1}\lambda_2^{h_2}\dots\lambda_m^{h_m}U$$

where h_i is the number of occurrences of i in the tableau. Thus U is invariant under the torus T if and only if all the indices $1, \dots, m$ appear exactly the same number of times. Finally on this ring of $SL(2) \times T$-invariants acts the symmetric group S_m and the $SL(2)$-invariants of the binary forms are identified to the S_m-invariants of this action.

3 Hilbert Series

3.1 Hilbert Series

In this section we shall develop a formula for the dimensions of the spaces of invariants and covariants in various degrees.

Given a representation ρ of a reductive group G on a vector space W, let R be the ring of polynomial functions on W.

We want to study the numbers (which we shall organize in a generating series):

$$d_i(\rho) := \dim R_i^G, \quad p_\rho(t) := \sum_{i=0}^{\infty} d_i(\rho)t^i. \tag{3.1.1}$$

We have already remarked in Chapter 8, §6 that a maximal compact subgroup K is Zariski dense; hence the G-invariants coincide with the K-invariants. We can thus apply the theory of characters of compact groups Chapter 8, §1.3.1 and Molien's theorem Chapter 9, §4.3.3 so that

$$p_\rho(t) = \int_K \det(1 - \rho(\gamma)t)^{-1}\, d\gamma$$

where $d\gamma$ is the normalized Haar measure on K.

One can transform this formula by the Weyl integration formula to an integration over a maximal torus T with coordinates z and normalized Haar measure dz:

$$p_\rho(t) = \int_T \det(1 - \rho(z)t)^{-1} A(z)\, dz$$

where $A(z)$ is the Weyl factor (Chapter 11, §9.1). In the case of $G = SL(2)$, $K = SU(2)$ the torus T is 1-dimensional and the Weyl factor is

$$A(z) = \frac{2 - z^2 - z^{-2}}{2}. \tag{3.1.2}$$

Let us start with invariants. We fix m and $S^m(V)$ the space of binary forms and let $R := \mathbb{C}[a_0, \dots, a_m]$, the ring of polynomial functions on $S^m(V)$. Denote by $p_m(t)$ the generating series on invariants and $p_m^c(t)$ the generating series for covariants.

The matrix $\rho(z)$ is diagonal with entries z^{-m+2k}, $k = 0, \dots, m$. Thus setting $z := e^{2\pi i \phi}$, the integral to be computed is

$$\int_0^1 \frac{1}{2}(2 - z^2 - z^{-2}) \prod_{k=0}^{m} (1 - z^{-m+2k} t)^{-1} d\phi,$$

or in the language of complex analysis:

$$p_m(t) = \frac{1}{2\pi i} \oint_T \frac{1}{2}(2 - z^2 - z^{-2}) \prod_{k=0}^{m} (1 - z^{-m+2k} t)^{-1} z^{-1}\, dz.$$

For covariants instead we have the extra factors:

$$p_m^c(t) = \frac{1}{2\pi i} \oint_T \frac{1}{2}(2 - z^2 - z^{-2})$$
$$\times \prod_{k=0}^{m} (1 - z^{-m+2k} t)^{-1} (1 - zt)^{-1} (1 - z^{-1} t)^{-1} z^{-1}\, dz.$$

Let us make the computations for invariants and for $m = 2p$ even. In this case one sees immediately that $\int_0^1 f(z^2)\, d\phi = \int_0^1 f(z)\, d\phi$, so we have

$$p_{2p}(t) = \frac{1}{2\pi i} \oint_T \frac{1}{2}(2 - z - z^{-1}) z^{-1} \prod_{k=-p}^{p} (1 - z^k t)^{-1}\, dz$$
$$= \frac{(-1)^p t^{-p}}{2\pi i (1 - t)} \oint_T \frac{1}{2}(2 - z - z^{-1}) z^{-1+p(p+1)/2}$$
$$\times \prod_{k=1}^{p} (1 - z^k t)^{-1} (1 - z^k t^{-1})^{-1}\, dz.$$

We apply partial fractions and the residue theorem. Set $\zeta_k := e^{2\pi i/k}$; we have

$$\prod_{k=1}^{p} (1 - z^k t)(1 - z^k t^{-1}) = \prod_{k=1}^{p} \prod_{j=0}^{k-1} (1 - \zeta_k^j t^{1/k} z)(1 - \zeta_k^{-j} t^{-1/k} z).$$

Let A denote the inverse of the product on the right-hand side. We expand

$$A = \sum_{k=1}^{p} \sum_{j=0}^{k-1} \frac{b_{kj}}{1 - \zeta_k^j t^{1/k} z} + \frac{c_{kj}}{1 - \zeta_k^{-j} t^{-1/k} z}$$

where the numbers b_{kj}, c_{kj} will be calculated later. For the integral p_{2p}, assuming $|t| < 1$ and $p \geq 2$ ($p = 1$ being trivial):

$$p_{2p} = \frac{(-1)^p}{2(1-t)t^p} \sum_{k=1}^{p} \sum_{j=0}^{k-1} c_{kj} (\zeta_k^j t^{1/k})^{p(p+1)/2} (2 - \zeta_k^j t^{1/k} - \zeta_k^{-j} t^{-1/k}). \tag{3.1.3}$$

We work now on the term

$$I_k := \sum_{k=1}^{p} \sum_{j=0}^{k-1} c_{kj} (\zeta_k^j t^{1/k})^{p(p+1)/2} (2 - \zeta_k^j t^{1/k} - \zeta_k^{-j} t^{-1/k}).$$

Recall that the partial fraction decomposition gives

$$\begin{aligned} c_{kj}^{-1} &= \prod_{h=1}^{p} \prod_{s=0}^{h-1} (1 - \zeta_h^s t^{\frac{1}{h}} \zeta_k^j t^{\frac{1}{k}})(1 - \zeta_h^{-s} t^{\frac{-1}{h}} \zeta_k^j t^{\frac{1}{k}}) \prod_{s=0}^{k-1} (1 - \zeta_k^s t^{\frac{1}{k}} \zeta_k^j t^{\frac{1}{k}}) \\ &\quad \times \prod_{s=0,\ s\neq j}^{k-1} (1 - \zeta_k^{-s} t^{\frac{-1}{k}} \zeta_k^j t^{\frac{1}{k}}) \\ &= \prod_{h=1,\ h\neq k}^{p} (1 - \zeta_k^{jh} t^{1+h/k})(1 - \zeta_k^{jh} t^{-1+h/k})(1 - t^2)k. \end{aligned} \tag{3.1.4}$$

In order to simplify the formula let us work in the formal field of Laurent series in $t^{1/N}$, where N is the least common multiple of the numbers $k = 1, \dots, p$. The automorphism $\sigma_N : t^{1/N} \to \zeta_N t^{1/N}$ induces a trace operator $\mathrm{Tr} := \frac{1}{N} \sum_{j=0}^{N-1} \sigma_N^j$ which has the property that, applied to a Laurent series in $t^{1/N}$, picks only the terms in t. In other words, $\mathrm{Tr}(t^a) = 0$ if a is not an integer, and $\mathrm{Tr}(t^a) = t^a$ if a is an integer. On the subfield of series in $t^{1/k}$ the operator $\mathrm{Tr} = \frac{1}{k} \sum_{j=0}^{k-1} \sigma_k^j$. Formulas 3.1.3 and 3.1.4 give $p_{2p} = \mathrm{Tr}(J)$ with

$$\begin{aligned} J &:= \frac{(-1)^p}{2(1-t)(1-t^2)t^p} \sum_{k=1}^{p} t^{p(p+1)/2k} (2 - t^{1/k} - t^{-1/k}) \\ &\quad \times \prod_{h=1,\ h\neq k}^{p} (1 - t^{1+h/k})^{-1} (1 - t^{-1+h/k})^{-1}. \end{aligned}$$

One can further manipulate this formula. Remark that

$$1 - t^{-1+h/k} = 1 - t^{(h-k)/k} = -t^{(h-k)/k}(1 - t^{(k-h)/k}).$$

If h runs from 1 to p and $h \neq k$, we have that $h + k$ runs from $k + 1$ to $k + p$ except $2k$, and if h runs from $k + 1$ to p, then $h - k$ runs from 1 to $p - k$. Finally when h runs from 1 to $k - 1$, we have that $k - h$ runs from 1 to $k - 1$. Then

$$\begin{aligned} &(1-t)(1-t^2) \prod_{h=1,\ h\neq k}^{p} (1 - t^{1+h/k})(1 - t^{-1+h/k}) \\ &= (-1)^{k-1} t^{(1-k)/2} \prod_{h=1}^{p+k} (1 - t^{h/k}) \prod_{h=1}^{p-k} (1 - t^{h/k}). \end{aligned}$$

In conclusion:

$$J = \frac{1}{2}(-1)^p \sum_{k=1}^{p} (-1)^{k-1} t^{E(p,k)} (t^{1/k} - 1)^2 \prod_{h=1}^{p+k} (1 - t^{h/k})^{-1} \prod_{h=1}^{p-k} (1 - t^{h/k})^{-1}$$

where $E(p,k) = (p-k+2)(p-k-1)/2k$.

Let us show now how the previous formulas can be used for an effective computation.

Let us write:

$$J = \frac{1}{2}(-1)^p \sum_{k=1}^{p} (-1)^{k-1} J_k, \quad J_k := \frac{H(p,k)}{\prod_{h=2}^{p+k}(1 - t^{h/k}) \prod_{h=2}^{p-k}(1 - t^{h/k})}$$

with $H(p,k) = t^{(p-k+2)(p-k+1)/2k}$ for $1 \le k \le p-1$ and $H(p,p) = (1 - t^{1/p})$. Since

$$(1 - t^{h/k})^{-1} = \left(\sum_{j=0}^{k-1} t^{jh/k}\right)(1 - t^h)^{-1},$$

we can write

$$J_k = \frac{H(p,k) \prod_{h=2}^{p+k} (\sum_{j=0}^{k-1} t^{jh/k}) \prod_{h=2}^{p-k} (\sum_{j=0}^{k-1} t^{jh/k})}{\prod_{h=2}^{p+k} (1 - t^h) \prod_{h=2}^{p-k} (1 - t^h)} = \frac{N_k}{D_k},$$

and get

(3.1.5) $$\operatorname{Tr}(J) = \frac{1}{2}(-1)^p \sum_{k=1}^{p} (-1)^{k-1} \frac{\operatorname{Tr}(N_k)}{D_k}.$$

Since N_k is an effectively given polynomial in $t^{1/k}$, we have that $\operatorname{Tr}(N_k)$ is an effectively computable polynomial in t.

We would like to express the Hilbert series in the form given by formula 1.1.3 of Chapter 12. For this we prove:

Proposition. *In formula 3.1.5, if p is even, the polynomial $g_e := \prod_{h=2}^{2p-1}(1 - t^h)$ is a common multiple of the D_k's.*

If p is odd, the polynomial $g_o := (1+t)\prod_{h=2}^{2p-1}(1 - t^h)$ is a common multiple of the D_k's.

Proof. For p odd note that

$$(1 - t^{-1/p}) \left(\sum_{j=0}^{p-1} t^{2j/p}\right) = -t^{-1/p}(1 - t) \left(\sum_{j=0}^{p-1} (-1)^j t^{j/p}\right).$$

For p even

$$(1-t^{-1/p})\left(\sum_{j=0}^{p-1} t^{2j/p}\right)\left(\sum_{j=0}^{p-1} t^{3j/p}\right)$$
$$= -t^{-1/p}(1-t^2)(1-t^{1/p}+t^{2/p})\left(\sum_{j=0}^{(p-2)/2}(-1)^j t^{6j/p}\right).$$

Hence when p is even:

$$J_p = -t^{-1/p}(1-t^{1/p}+t^{2/p})\left(\sum_{j=0}^{(p-2)/2}(-1)^j t^{6j/p}\right)$$
$$\times \prod_{h=4}^{2p-1}\left(\sum_{j=0}^{p-1} t^{jh/p}\right)\Bigg/\prod_{h=2}^{2p-1}(1-t^h),$$

while when p is odd:

$$J_p = -t^{-1/p}\left(\sum_{j=0}^{p-1}(-1)^j t^{j/p}\right)\prod_{h=3}^{2p-1}\left(\sum_{j=0}^{p-1} t^{jh/p}\right)\Bigg/(1+t)\prod_{h=2}^{2p-1}(1-t^h).$$

To finish we have to prove that the denominators D_k for $k < p$ divide the denominator found for J_p. So, let Φ_d denote the cyclotomic polynomial for primitive d^{th} roots of 1, and $t^h - 1 = \prod_{d \mid h} \Phi_d$. Denote finally by $[a/b]$ the integral part of the fraction $a/b,\ a, b \in \mathbb{N}$. Then

$$D_k = \prod_{h=2}^{p+k}(1-t^h)\prod_{h=2}^{p-k}(1-t^h) = \Phi_1^{2p-2}\prod_{d\geq 2}\Phi_d^{[(p+k)/d]+[(p-k)/d]}$$

$$g_e = \Phi_1^{2p-2}\prod_{d\geq 2}\Phi_d^{[(2p-1)/d]}, \qquad g_o = \Phi_1^{2p-2}\Phi_2^{[(2p-1)/2]}\prod_{d\geq 3}\Phi_d^{[(2p-1)/d]} \qquad \square$$

The numerator of the Hilbert series can at this point be made explicit. Computer work, done for forms of degree ≤ 36, gives large numbers and some interesting facts about which we will comment in the next section.

4 Forms and Matrices

4.1 Forms and Matrices

There is even another method to find explicit invariants of binary forms, discovered by Hilbert.

It is based on the Clebsch–Gordan formula

$$S^m(V) \otimes S^n(V) = \bigoplus_{i=0}^{\min m,n} S^{m+n-2i}(V).$$

If we apply it when $m = n$, we can take advantage of the fact that $S^m(V) \equiv S^m(V)^*$ and thus obtain

$$\mathrm{End}(S^m(V)) = S^m(V) \otimes S^m(V)^* \equiv S^m(V) \otimes S^m(V) = \bigoplus_{i=0}^{m} S^{2i}(V).$$

Therefore the forms $S^{2i}(V)$ can be embedded in an $SL(2)$-equivariant way into $\mathrm{End}(S^m(V))$ for all $m \geq i$. In particular, the coefficients of the characteristic polynomial of elements of $\mathrm{End}(S^m(V))$, restricted to $S^{2i}(V)$, are $SL(2)$-invariants. The identification $S^m(V) \equiv S^m(V)^*$ is given by an invariant nondegenerate form which, for m odd, is symplectic while for m even, it is symmetric (Chapter 5, §3.7). In both cases, on $\mathrm{End}(S^m(V))$ we have an $SL(2)$-invariant involution $*$ and $(a \otimes b)^* = \epsilon(b \otimes a)$ where $\epsilon = -1$ in the symplectic and $\epsilon = 1$ in the orthogonal case. It is interesting to see how the decomposition $S^m(V) \otimes S^m(V) = \bigoplus_{i=0}^{m} S^{2i}(V)$ behaves under the symmetry $\tau : a \otimes b \to b \otimes a$. We have:

Proposition. *$\tau = (-1)^i$ on $S^{2(m-i)}(V)$.*

Proof. Since τ is $SL(2)$ equivariant and has only eigenvalues ± 1 on each space $S^{2i}(V)$ which is an irreducible representation of $SL(2)$, it must be either 1 or -1. To determine the sign, recall the formula 2.1.2 of transvection, which in our case is $(a_x^m, b_y^m)_i = (a, b)^i a_x^{m-i} b_x^{m-i}$ and which can be interpreted as the image of $a_x^m \otimes b_x^m$ in $S^{2(m-i)}(V)$ under the canonical projection. We have by equivariance

$$(-1)^i (a, b)^i a_x^{m-i} b_x^{m-i} = (b, a)^i b_x^{m-i} a_x^{m-i} = (b_x^m, a_y^m)_i = \tau((a, b)^i a_x^{m-i} b_x^{m-i}). \qquad \square$$

We obtain:

Corollary. *$S^{2(m-i)}(V) \subset S^m(V)$ is formed by symmetric matrices when m and i are odd or m and i are even, otherwise it is formed by antisymmetric matrices.*

Thus one method to find invariants is to take coefficients of the characteristic polynomials of these matrices. When one starts to do this one discovers that it is very hard to relate invariants given by different matrix representations. In any case these computations and the ones on Hilbert series suggest a general conjecture with which we want to finish this book, showing that even in the most ancient and basic themes there are difficult open problems. The problem is the following. From Proposition 6.1 we have seen that the Hilbert series of binary forms, in case the forms are of degree $4k$, a multiple of 4, is of the form

$$f(t) / \prod_{i=2}^{4k-1} (1 - t^i).$$

When one computes them (and one can do quite a lot of computations by computer) one discovers that for $4k \leq 36$, the coefficients of $f(t)$ are nonnegative. Recalling the theory of Cohen–Macaulay algebras this suggests that there may be a regular sequence of invariants of degree i, $2 \leq i \leq 4k - 1$. One way in which such a sequence could arise is as coefficients of the characteristic polynomial of a corresponding matrix.

In particular when we embed $S^{4k}(V) \subset \mathrm{End}(S^{4k-2}(V))$ we have (since the matrices we obtain have order $4k - 1$ and trace 0), exactly $4k - 2$ coefficients. One may attempt to guess that these coefficients form a regular sequence. There is even a possible geometric way of checking this. Saying that in a Cohen–Macaulay graded ring of dimension h, h elements form a regular sequence is equivalent to saying that their common zeros reduce to the point 0. When we are dealing with invariants this is equivalent to saying that as functions of $S^{4k}(V)$ they define the set of unstable points, that is the set on which all invariants vanish. By Chapter 14, §4.1 a binary form is unstable if and only if one of its zeroes has multiplicity $> n/2$. On the other hand, for a matrix x the coefficients of its characteristic polynomial are 0 if and only if the matrix is nilpotent. So, in the end, the question is: if the endomorphism on $S^{4k-2}(V)$ induced by a form on $S^{4k}(V)$ is nilpotent, is the form unstable?

This seems to be very hard to settle. Even if it is false it may still be true that there is a regular sequence of invariants of degree i, $2 \leq i \leq 4k - 1$.