# Calculation of normal forms

Lay May Yeap

June 2004

## 1 Algebraic Structure and Syzygies

## 2 Normal Form Revisited

The homological equation $D_x F(x) L_0^* x - L_0^* F(x) = 0$ (where $D_x$ is the differential operator with respect to $x$) fully characterizes the normal form $F(x) = \begin{pmatrix} F_0 \\ \vdots \\ F_n(x) \end{pmatrix}$. Thus, the homological operator

$$H_x = (L_0^* x) \cdot D_x \tag{1}$$

is an essential ingredient in computation of normal forms.

The equation

$$H_x f(x) = 0 \tag{2}$$

is a first order PDE that can be solved using the method of characteristics. In particular, we can obtain $n-1$ functionally independent first integrals such that any solution $f(x)$ can be written in terms of these $n-1$ first integrals. However, our goal is a bit different. We seek $f(x)$ that is polynomial in $x$.

The fact that we only consider $f(x)$ that is polynomial, also justifies a few technicalities in the employ of method of characteristic system. In computation of normal form, often time, the operator $H_x$ becomes singular at certain $x$. For instance, suppose $H_x = x_1 \frac{\partial}{\partial x_2}$, the operator becomes singular when $x_1 = 0$. This singular set (i.e. the set of $x$ such that $H_x = 0$) is of measure zero. In fact, the complement of this singular set is dense. Since $f$ is a polynomial, $f$ is obviously continuous in this complement set. If we obtain a representation for polynomial solutions $f(x)$ on the complement of this singular set, we can extend it to the singular set.

The question we wish to explore is, how do we represent $f(x)$ in terms of a set of functionally independent first integrals of equation (2)? Can we always obtain a polynomial representation for $f$ in terms of these first integrals? In general, the answer to the latter question is negative. In fact, as suggested in ([4]), in general, $f$ is rational in the new variables defined by those chosen first integrals.

**Example 1.**

$$L_0 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \qquad x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}.$$

*Then*

$$H_x f(x) = \left( x_1 \frac{\partial}{\partial x_2} + x_2 \frac{\partial}{\partial x_3} + x_3 \frac{\partial}{\partial x_4} \right) f(x) = 0.$$

*The 3 independent first integrals can be chosen to be* $u_1 = x_1, u_2 = x_2^2 - 2x_1x_3, u_3 = x_2^3 + 3x_1^2x_4 - 3x_1x_2x_3$. *Then,* $f$ *can be expressed as*

$$f(x) = \frac{P(u_1, u_2, u_3)}{u_1^a}$$

*where* $P$ *is polynomial in its variable.*

*Consider*

$$u_1^a f(x) = P(u_1, u_2, u_3).$$

*When* $u_1 \to 0$, *we must have* $P(0, u_2, u_3) = 0$. *If* $u_2, u_3$ *remain functionally independent, then* $P(0, u_2, u_3) = 0$ *for all possible* $u_2, u_3$ *implies* $u_1$ *is a factor of* $P$. *Hence,* $f$ *can be written as*

$$f(x) = \frac{\tilde{P}(u_1, u_2, u_3)}{u_1^{a-1}}.$$

*Doing this inductively will prove that* $f$ *is actually polynomial in all* $u_1, u_2, u_3$.

*However, in this case,* $u_2 = x_2^2$, $u_3 = x_2^3$ *when* $u_1 = x_1 \to 0$. *In other words,* $u_2$, $u_3$ *are not functionally independent. In fact,* $u_2^3 - u_3^2 = 0$. *Hence, we cannot conclude that* $u_1$ *is a factor of* $P$ *from the equation* $P(0, u_2, u_3) = 0$. *It is possible that* $u_2^3 - u_3^2$ *is a factor for* $P$ *instead. Therefore, we shall continue to regard* $f$ *as rational in* $u$*'s.*

We shall refer to the new variables defined by first integrals of equation (2) as characteristic variables. The rationality of $f$ in terms of the characteristic variables, is a common phenomenon for sufficiently high codimension normal forms. Because reversibility reduces the effective codimension, this phenomenon arises even for codimension 2 cases.

Let $U = \{u_1, u_2, \cdots, u_{n-1}\}$ be the set of characteristic variables. In many cases where $f$ is rational in $u$'s, there exists at least a rational function in a subset of $U$ of the form

$$u_s = \frac{P_s(u_{i_1}, u_{i_2}, \cdots, u_{i_k})}{u_{d_1}^{\alpha_1} u_{d_2}^{\alpha_2} \cdots u_{d_r}^{\alpha_r}}, \tag{3}$$

where $\{u_{d_j}\} \subset \{u_{i_j}\} \subset U$, such that $u_s$ is polynomial in $x$ and $P_s$ vanishes as some of the $u_{d_j} \to 0$, and the numerator and denominator have no common factor. We say that the set $\{u_{i_1}, \cdots, u_{i_k}\}$ is rationally dependent. Note that $u_s$ solves equation (2). The inclusion of $u_s$ into the set of characteristic variables would allow $f$ to be expressed as a polynomial in terms of this new set of variables. The inclusion of $u_s$ introduces a *syzygy* in the set of characteristic variables. In general, there may be more than one such $u_s$ and therefore more than one syzygy.

**Definition 1.** *A syzygy of a set of linearly independent variables $\{w_1, w_2, \cdots, w_n\}$ is a polynomial relation among the variables such that no $w_i$ can be written as a polynomial in the rest of the variables.*

**Example 2.** *For the case of 4 zeros, we have*

$$u_s = \frac{u_3^2 - u_2^3}{u_1^2} = -3x_2^2x_3^2 + 8x_1x_3^3 + 6x_2^3x_4 - 18x_1x_2x_3x_4 + 9x_1^2x_4^2.$$

*This can be observed from the functional relation between $u_2$ and $u_3$ when $u_1 \to 0$, as discussed in example (1).*

*One can easily check that $u_s$ solves equation (2). Hence, a syzygy in this case would be*

$$u_1^2 u_s - u_3^2 + u_2^3 = 0.$$

The existence of syzygies implies that the polynomial representation for $f$ in terms of the characteristic variables cannot be unique. To obtain a minimal representation for $f$, we need to mod out the ideal generated by the syzygies. Suppose the syzygies are in the form

$$\begin{aligned} u_j^\alpha =& u_j^{\alpha-1} P_1^j(u_{i_1}, u_{i_2}, \cdots, u_{i_k}) + u_j^{\alpha-2} P_2^j(u_{i_1}, u_{i_2}, \cdots, u_{i_k}) + \cdots + P_\alpha^j(u_{i_1}, u_{i_2}, \cdots, u_{i_k}), \\ & j \neq i_l \, \forall l = 1, 2, \cdots, k, \end{aligned} \tag{4}$$

where $\{u_j, u_{i_1}, \cdots, u_{i_k}\} = U \bigcup \{u_s\}$, $\{u_s\}$ is the set of rational functions of $u \in U$ as in equation (3) that yields the syzygies. Each $P^j$ is polynomial in its variables. Then the "modding out" process is simply a division algorithm. In other words

$$\begin{aligned} f(x) =& \Big( u_j^\alpha - u_j^{\alpha-1} P_1^j(u_{i_1}, \cdots, u_{i_k}) - u_j^{\alpha-2} P_2^j(u_{i_1}, \cdots, u_{i_k}) - \cdots - P_\alpha^j(u_{i_1}, \cdots, u_{i_k}) \Big) \\ & Q(u_{i_1}, \cdots, u_{i_k}) + u_j^{\alpha-1} R_1(u_{i_1}, \cdots, u_{i_k}) + u_j^{\alpha-2} R_2(u_{i_1}, \cdots, u_{i_k}) + \cdots \\ & + R_0(u_{i_1}, \cdots, u_{i_k}) \\ =& u_j^{\alpha-1} R_{\alpha-1}(u_{i_1}, \cdots, u_{i_k}) + u_j^{\alpha-2} R_{\alpha-2}(u_{i_1}, \cdots, u_{i_k}) + \cdots + R_0(u_{i_1}, \cdots, u_{i_k}) \end{aligned} \tag{5}$$

where $Q, R_0, \cdots, R_{\alpha-1}$ are polynomials in their variables and $R_0, \cdots, R_{\alpha-1}$ are the remainder terms. The first term drops out because of the syzygy.

**Example 3.** *Consider example (2) again. The syzygy is*

$$u_3^2 = u_1^2 u_s + u_2^3.$$

*We shall first show that $f$ is indeed a polynomial in $u_1, u_2, u_3, u_s$. By grouping the even and odd parts of $u_3$, we reexpress $f$ from example (1) as*

$$\begin{aligned} f(x) =& \frac{P_1(u_1, u_2, u_3^2) + u_3 P_2(u_1, u_2, u_3^2)}{u_1^a} \\ =& \frac{\tilde{P}_1(u_1, u_2, u_s) + u_3 \tilde{P}_2(u_1, u_2, u_s)}{u_1^a} \end{aligned}$$

*by replacing $u_3^2$ by $u_1^2 u_s - u_2^3$ given by the syzygy. To show that this division yields a polynomial for $f$ in terms of $u$'s, we use argument similar to that outlined in example (1). First, we write*

$$u_1^a f(x) = \tilde{P}_1(u_1, u_2, u_s) + u_3 \tilde{P}_2(u_1, u_2, u_s). \tag{6}$$

*When $u_1 \to 0$, $u_2 = x_2^2, u_3 = x_2^3, u_s = -3x_2^2 x_3^2 + 6x_2^3 x_4$. Note that $u_2$ and $u_s$ remain functionally independent, while $u_3 = (\sqrt{u_2})^3$. Equation (6) now reads*

$$\tilde{P}_1(0, u_2, u_s) + (\sqrt{u_2})^3 \tilde{P}_2(0, u_2, u_s) = 0.$$

*This implies $\tilde{P}_1(0, u_2, u_s) = 0$ and $\tilde{P}_2(0, u_2, u_s) = 0$. Since $u_2, u_s$ remain functionally independent, $\tilde{P}_i(0, u_2, u_s) = 0$, $i = 1, 2$ implies $u_1$ is an explicit factor for $\tilde{P}_i$. Hence, we can write*

$$f(x) = \frac{\tilde{\tilde{P}}_1(u_1, u_2, u_s) + u_3 \tilde{\tilde{P}}_2(u_1, u_2, u_s)}{u_1^{a-1}}.$$

*Applying this argument inductively proves $f$ as a polynomial in $u_1, u_2, u_s$ and at most linear in $u_3$.*

*Now, suppose we know that $f$ is polynomial in $u_1, u_2, u_3, u_s$, we can divide it by the expression in $u$ given by the syzygy:*

$$\begin{aligned} f(x) =& Poly(u_1, u_2, u_3, u_s) \\ =& (u_3^2 - u_1^2 u_s - u_2^3) Q(u_1, u_2, u_3, u_s) + u_3 R_1(u_1, u_2, u_s) + R_0(u_1, u_2, u_s) \end{aligned}$$

*where $Q, R_0, R_1$ are polynomials in their variables, $R_0, R_1$ are the remainder terms. Since the syzygy gives $u_3^2 - u_1^2 u_s - u_2^3 = 0$, the first term drops out. Hence,*

$$f(x) = u_3 R_1(u_1, u_2, u_s) + R_0(u_1, u_2, u_s)$$

*which is exactly the same form we obtain via direct computation in the previous paragraph.*

When there are more than one syzygy, there is an ambiguity of ordering in the division algorithm. For this, we need to turn to Groebner bases. Groebner bases are a general purpose method for multivariate polynomial computations. First, we need to specify a total order $\prec$ on monomials $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} \in k[x_1, x_2, \cdots, x_n]$ where $k$ is the polynomial ring generated by $x_1, \cdots, x_n$ over the field $k$. $\prec$ is a monomial order if for any $m_1, m_2, m_3$, $1 \preceq m_1$ and $m_1 \preceq m_2 \Rightarrow m_1 \cdot m_3 \preceq m_2 \cdot m_3$. For example, we can choose an ordering on $k[x_1, x_2, x_3]$ such that $1 \prec x_1 \prec x_1^2 \prec \cdots \prec x_2 \prec x_2 x_1 \prec x_2 x_1^2 \prec \cdots \prec x_3 \prec x_3 x_1 \prec x_3 x_1^2 \prec \cdots$.

There are several useful standard monomial orderings.

**Definition 2.** *(Lexicographic Order)*
*Let $\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_n)$ and $\beta = (\beta_1, \beta_2, \cdots, \beta_n) \in (\mathbb{Z}^n)^+$. $\alpha \succ_{lex} \beta$ if, in the vector difference $\alpha - \beta \in \mathbb{Z}^n$, the left-most nonzero entry is positive. We say $x^\alpha \succ_{lex} x^\beta$ if $\alpha \succ_{lex} \beta$.*

**Example 4.** *Suppose $\alpha = (1, 2, 0)$ and $\beta = (0, 3, 4)$. Then, $\alpha \succ_{lex} \beta$ since $\alpha - \beta = (1, -1, -4)$.*

**Definition 3.** *(Graded Lex Order)*
*Let $\alpha, \beta \in (\mathbb{Z}^n)^+$. Then, $\alpha \succ_{grlex} \beta$ if*

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i, \quad \text{or} \quad |\alpha| = |\beta| \text{ and } \alpha \succ_{lex} \beta.$$

**Example 5.**

1. *Suppose* $\alpha = (1,2,3)$ *and* $\beta = (3,2,0)$. *Then,* $\alpha \succ_{grlex} \beta$ *since* $|(1,2,3)| = 6 > |(3,2,0)| = 5$.

2. *Suppose* $\alpha = (1,2,4)$ *and* $\beta = (1,1,5)$. *Then,* $\alpha \succ_{grlex} \beta$ *since* $|(1,2,4)| = 7 = |(1,1,5)| = 7$ *but* $\alpha - \beta = (0,1,-1)$, *i.e.* $\alpha \succ_{lex} \beta$.

**Definition 4.** *(Graded Reverse Lex Order)*
*Let* $\alpha, \beta \in (\mathbb{Z}^n)^+$. *Then* $\alpha \succ grevlex\beta$ *if*

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i, \quad or \ |\alpha| = |\beta|$$

*and in* $\alpha - \beta \in \mathbb{Z}^n$, *the right-most nonzero entry is negative.*

**Example 6.**

1. *Suppose* $\alpha = (2,5,1)$ *and* $\beta = (2,3,2)$. *Then,* $\alpha \succ_{grevlex} \beta$ *since* $|\alpha| = 8 > |\beta| = 7$.

2. *Suppose* $\alpha = (1,5,2)$ *and* $\beta = (4,1,3)$. *Then,* $|\alpha| = 8 = |\beta| = 8$ *and* $\alpha - \beta = (-3,4,-1)$. *Hence,* $\alpha \succ_{grevlex} \beta$.

Fixing an monomial order $\prec$ on $k[x_1, x_2, \cdots, x_n]$, we denote the largest monomial of a polynomial $f \in k[x_1, x_2, \cdots, x_n]$ by $init(f)$ – the initial monomial of $f$. For an ideal $I \subset k[x_1, x_2, \cdots, x_n]$, the innitial ideal is the ideal generated by the initial monomials of all polynomials in $I$, i.e. $init(I) :=< \{init(f) \,|\, f \in I\} >$ . An ideal generated by monomials, e.g. $init(I)$ is call a monomial ideal. The monomials $m \notin init(I)$ are said to be *standard*.

**Definition 5.** *A finite set* $\mathcal{G} := \{g_1, g_2, \cdots, g_s\}$ *of an ideal* $I$ *is a* Groebner basis *for* $I$ *if* $init(I) =< \{init(g_1), init(g_2), \cdots, init(g_s)\} >$ . *Moreover,* $\mathcal{G}$ *is called* reduced *if* $init(g_i)$ *dose not divide any monomial occuring in* $g_j$ *for* $j \neq i$.

Many mathematical softwares, e.g. *MAPLE, Mathematica* have in-built function to compute Groebner basis. Such programs take a finite set $\mathcal{S} \subset \mathbb{C}[\mathbf{x}]$ and output a reduced Groebner basis $\mathcal{G}$ for the ideal $< \mathcal{S} >$ using Buchberger's algorithm introduced in his 1965 Ph.D. thesis, written at the University of Innsbruck (Tyrol, Austria) under the supervision of Wolfgang Groebner [1, 3].

Groebner basis has many applications aside from dealing with the "ordering problem" in division algorithm. Nonetheless, we shall present a simple example to demonstrate the its application in multivariable division, i.e.

to rewrite every polynomial modulo $< \mathcal{S} >$ as a $\mathbb{C}$-linear combination of standard monomials.

**Example 7.** *First, we specify an ordering – a lexicographic ordering induced by* $x \prec y$. *That is,* $1 \prec x \prec x^2 \prec \cdots \prec y \prec yx \prec yx^2 \prec \cdots$. *Suppose we want to divide the polynomial* $P = y^4 + y^3$ *by* $\mathcal{S} = \{y^2 + x^2 - 1, 3xy - 1\}$. *The Groebner basis for* $\mathcal{S}$ *is* $\mathcal{G} = \{y + 3x^3 - 3x, 9x^4 - 9x^2 + 1\}$. *Dividing* $P$ *by* $\mathcal{S}$ *is equivalent to dividing* $P$ *by* $\mathcal{G}$, *except* $\mathcal{G}$ *allows division by its elements in arbitrary order while yielding a unique residue. Note that the standard monomials for* $\mathcal{G}$ *is* $x_3, x_2, x, 1$. *Moding* $P$ *by* $\mathcal{G}$ *leaves the residue* $27x^3 + 9x^2 - 24x - 8$ *which is precisely* $\mathbb{C}$*-linear combination of the standard monomials.*

In the cases where syzygies are in the form given by (4), then $f$ *can be expressed in terms of* $u$*'s algebraicly and integrally.* Unfortunately, syzygies do not always emerge in such desirable form. It is therefore not obvious how a division algorithm can be employed in these cases. To account for this difficulty, we use ideas from classical invariant theory to obtain an alternate derivation for normal forms.

In the next section (3), we reinterpret the above ideas in an algebraic language. In the section (4), we provide a summary of ideas from classical invariant theory. We then explain a connection of these ideas with the computation of normal forms in section (5). And lastly, in section (6) we show an alternate derivation of normal forms using the ideas from invariant theory.

## 3 Ring of Polynomial Invariants and Syzygy Ideals

The set of $S = \{u = P(x) \,|\, H_x u = 0,\ P \text{ is a polynomial in its variables}\}$ forms a ring. That is to say if $u_1, u_2 \in S$, so are $u_1 + u_2$ and $u_1 \cdot u_2$. The fact that $S$ is a ring follows immediately from linearity of $H_x$ and product rule of differential operators. Since $u$ is an invariant for equation (2) by definition, we shall refer to $S$ as a ring of polynomial invariants.

Let $k[u_1, u_2, \cdots], \quad u_i \in S \quad \forall i$, be the polynomial ring generated by the $u$'s over field $k$. $k$ can be $\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Z}$ etc. depending on context. Clearly, $S \subset k[u_1, u_2, \cdots]$. It is also obvious that $k[u_1, u_2, \cdots] \subset S$ since every polynomial in $u_1, u_2, \cdots$ is a polynomial in $x$ and solves equation (2). Hence, $S = P[u_1, u_2, \cdots]$.

The first question is, does $k[u_1, u_2, \cdots]$ have a finite basis? This question can be answered positively using Hilbert's Finite Basis theorem [6, 2]. We

shall investigate this question in the section (5). Suppose $\tilde{u}_1, \tilde{u}_2, \cdots \tilde{u}_m$ is a finite basis, i.e. no $\tilde{u}_i$ can be written as a polynomial in the rest of the $\tilde{u}_j$, $j \neq i$, and this set generates the ring $k[u_1, u_2, \cdots]$. Dropping the tildes, let $k[u_1, \cdots, u_m]$ be the ring of polynomial generated by $u_1, \cdots, u_m$ over $k$. Then, there is a natural ring homomorphism $\phi : k[u_1, u_2, \cdots, u_m] \to S$ given by the substitution of $u$'s in terms of $x$'s. Hence, every polynomial solution to equation (2) is uniquely representable in $k[u_1, u_2, \cdots, u_m]/\{\ker(\phi)\}$.

$\ker(\phi) = \{Poly(u_1, u_2, \cdots, u_m) \,|\, \phi(Poly(u_1, \cdots u_m)) = 0\}$. Hence, every element in $\ker(\phi)$ yields a syzygy. Also, for any $p \in \ker(\phi)$ and $q \in k[u_1, u_2, \cdots, u_m]$, clearly $\phi(pq) = 0$ since $\phi(pq) = \phi(p)\phi(q)$ and $\phi(p) = 0$. Hence, $\ker(\phi)$ forms an ideal. We shall refer to it as the *syzygy ideal*.

The question we are trying to answer is therefore rephrased into finding the general representation for $k[u_1, u_2, \cdots, u_m]/\{\ker(\phi)\}$.

# 4 Classical Invariant Theory

Before we use the ideas from classical invariant theory to investigate the representation of $k[u_1, u_2, \cdots, u_m]/\{\ker(\phi)\}$, we shall first equip ourselves with the basic theory of algebraic invariants. We shall present a summary of ideas that are relevent to us. For a more complete exposition, one shall refer to [6, 11].

In this section, the notation used is local to discussion of Classical Invariant Theory. It is not carried from, or over to, problems of reversible normal forms or elliptical instability.

**Definition 6.** *An m-ary, n form is a homogeneous polynomial of order n in m variables. We denote such a form by* $\mathcal{F}^{(n)}(x_1, x_2, \cdots, x_m)$.

Of particular interest to us is the binary $n$ form

$$\mathcal{F} = \mathcal{F}^{(n)}(x_1, x_2) = a_0 x_1^n + \binom{n}{1} a_1 x_1^{n-1} x_2 + \binom{n}{2} a_2 x_1^{n-2} x_2^2 + \cdots + a_n x_2^n. \quad (7)$$

We shall henceforth focus our discussion on binary forms.

A linear transformation

$$\begin{aligned} x_1 &= \alpha_{11} x_1' + \alpha_{12} x_2' \\ x_2 &= \alpha_{21} x_1' + \alpha_{22} x_2' \end{aligned}$$

produces a transformed binary $n$ form $\mathcal{F}'(x_1', x_2')$. Note that the transformed form has the same order as the original form.

An immediate task is to describe common property for all these forms that are "equivalent" under linear transformations. This leads us to examine *invariants* and *covariants* of the form $\mathcal{F}$.

**Definition 7.** *Let $\delta = \alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21}$ be the determinant of the linear transformation. An invariant of the base form $\mathcal{F}$ is a polynomial $\mathcal{I}$ defined by*

$$\mathcal{I}(a'_0, a'_1, \cdots, a'_n) = \delta^p \mathcal{I}(a_0, a_1, \cdots, a_n) \tag{8}$$

*where $p \in \mathbb{Z}$, $a_0, \cdots, a_n$ are the coefficients of $\mathcal{F}$ and $a'_0, \cdots, a'_n$ are the coefficients of $\mathcal{F}'$.*

**Definition 8.** *A covariant of the base form $\mathcal{F}$ is a polynomial $\mathcal{C}$ defined by*

$$\mathcal{C}(a'_0, a'_1, \cdots, a'_n; x'_1, x'_2) = \delta^p \mathcal{C}(a_0, a_1, \cdots, a_n; x_1, x_2) \tag{9}$$

*where $\delta$ is the determinant of the linear transformation, $p \in \mathbb{Z}$, $a_0, a_1, \cdots, a_n$ and $x_1, x_2$ are respectively the coefficients and the variables of $\mathcal{F}$, and, $a'_0, a'_1, \cdots, a'_n$ and $x'_1, x'_2$ are respectively the coefficients and variables of $\mathcal{F}'$.*

The power of the coefficients $a_0, a_1, \cdots, a_n$ is called the degree of the invariant while the power of the variables $x_1, x_2$ is the order of the invariant or covariant. Thus, invariants are also covariants of order 0. Invariants and covariants together form the *invariant system* and their characterizing property is called the *invariant property.*

## 4.1 Invariant Property

To obtain the invariant property, we need to understand the behavior of invariants and covariants under linear transformation. First, it can be shown that every linear transformation of binary forms can be composed of the following three types of linear transformations:

$$\begin{aligned} x_1 &= \kappa x'_1, \\ x_2 &= \lambda x'_2. \end{aligned} \tag{10}$$

$$\begin{aligned} x_1 &= x'_1 + \mu x'_2, \\ x_2 &= x'_2. \end{aligned} \tag{11}$$

$$\begin{aligned} x_1 &= x'_1 \\ x_2 &= \nu x'_1 + x'_2 \end{aligned} \tag{12}$$

Applying the first type of transformation (10) to the binary form (7), the coefficients are tranformed into

$$a'_i = a_i \kappa^{n-i} \lambda^i$$

The transformation determinant here is $\delta = \kappa\lambda$.

An invariant of form (7) $\mathcal{I}(a_0, a_1, \cdots, a_n) = \sum Z_{\nu_0\nu_1\cdots\nu_n} a_0^{\nu_0} a_1^{\nu_1} \cdots a_n^{\nu_n}$ becomes

$$\begin{aligned}\mathcal{I}(a_0', a_1', \cdots, a_n') =& \sum \Big( Z_{\nu_0\nu_1\cdots\nu_n} a_0^{\nu_0} a_1^{\nu_1} \cdots a_n^{\nu_n} \kappa^{(n\nu_0+(n-1)\nu_1+\cdots+(n-i)\nu_i+\cdots\nu_{n-1})} \\ & \lambda^{(\nu_1+\cdots+i\nu_i+\cdots+n\nu_n)} \Big) \\ =& \kappa^p \lambda^p \sum Z_{\nu_0\nu_1\cdots\nu_n} a_0^{\nu_0} a_1^{\nu_1} \cdots a_n^{\nu_n} \\ & \text{since this should equals } \delta^p \mathcal{I}(a_0, a_1, \cdots, a_n)\end{aligned}$$

This yields the identities

$$\begin{aligned} n\nu_0 + (n-1)\nu_1 + \cdots + (n-i)\nu_i + \cdots \nu_{n-1} =& p \\ \nu_1 + \cdots + i\nu_i + \cdots + n\nu_n =& p \end{aligned}$$

Adding these, we obtain

$$n(\nu_0 + \nu_1 + \cdots + \nu_n) = 2p.$$

We define the degree as $g = \nu_0 + \nu_1 + \cdots + \nu_n$ and weight $\nu_1 + 2\nu_2 + \cdots + n\nu_n$. Then, we have

$$\begin{aligned} \nu_1 + 2\nu_2 + \cdots + n\nu_n =& p \\ ng =& 2p \end{aligned}$$

We summarize the result above in the following theorem:

**Theorem 1.** *Every invariant of a binary form is homogeneous in the coefficients, and each term has degree*

$$g = \frac{2p}{n}$$

*where $p$ is the exponent of the transformation determinant $\delta$, by which $\mathcal{I}$ changes under substitution of the transformed coefficients $a_0', \cdots, a_n'$. Also, all terms are isobaric, i.e. have the same weight, that equals $p$.*

We can use the exact same idea to deduce analogous property for covariants. Note, however, that there is no loss of generality to assume that covariants are homogeneous in variables $x_1, x_2$. If the covariants are not homogeneous in $x_1, x_2$, the defining property $\mathcal{C}(a_0', \cdots, a_n'; x_1', x_2') = \delta^p \mathcal{C}(a_0, \cdots, a_n; x_1, x_2)$ still has to hold for each homogeneous part.

The analogous property for covariant is summarized below:

**Theorem 2.** *Suppose covariant of a binary form is*

$$\mathcal{C} = C_0 x_1^m + \binom{n}{1} C_1 x_1^{m-1} x_2 + \cdots + C_m x_2^m.$$

*Then all terms of* $C_0, \cdots, C_m$ *have the same degree* $g$ *and weights* $p, p+1, \cdots, p+m$ *respectively. The weight of* $C_0$ *is the weight of the covariant and it determines the power of transformation determinant* $\delta$ *by which the covariant changes under the transformation. The order of covariant is*

$$m = ng - 2p.$$

Applying the second type of linear transformation (11) to a binary form (7) changes the coefficients by

$$a_i' = a_i + \binom{i}{1} \mu a_{i-1} + \binom{i}{2} \mu^2 a_{i-2} + \cdots + \mu^i a_0.$$

The transformation determinant is $\delta = 1$.

An invariant has to satisfy the equation $\mathcal{I}(a_0', \cdots, a_n') = \mathcal{I}(a_0, \cdots, a_n)$ for all $\mu$. Differentiating both sides with respect to $\mu$, we obtain

$$\frac{\partial \mathcal{I}(a')}{\partial a_0'} \frac{da_0'}{d\mu} + \frac{\partial \mathcal{I}(a')}{\partial a_1'} \frac{da_1'}{d\mu} + \cdots \frac{\partial \mathcal{I}(a')}{\partial a_n'} \frac{da_n'}{d\mu} = 0.$$

But, we also have $\frac{da_i'}{d\mu} = i a_{i-1}'$. The above differential equation becomes

$$\frac{\partial \mathcal{I}(a')}{\partial a_0'} \cdot 0 + \frac{\partial \mathcal{I}(a')}{\partial a_1'} \cdot a_0' + \cdots \frac{\partial \mathcal{I}(a')}{\partial a_n'} \cdot n a_{n-1}' = 0.$$

However, $\mathcal{I}(a')$ depends on $a'$ in exactly the same way as $\mathcal{I}(a)$ deepens on $a$. We can therefore remove the "primes" in the above differential equation and arrive at the following theorem:

**Theorem 3.** *An invariant of a binary form satisfies the differential equation*

$$\mathbf{D}\mathcal{I} := a_0 \frac{\partial \mathcal{I}}{\partial a_1} + 2a_1 \frac{\partial \mathcal{I}}{\partial a_2} + \cdots + n a_{n-1} \frac{\partial \mathcal{I}}{\partial a_n} = 0. \tag{13}$$

A similar analysis for covariant yields the following

**Theorem 4.** *Every covariant* $\mathcal{C}$ *of a binary form satisfies the differential equation*

$$\mathbf{D}\mathcal{C} = x_2 \frac{\partial \mathcal{C}}{\partial x_1}. \tag{14}$$

*That is to say* $\mathbf{D}C_i = iC_{i-1}$. *In particular, the source of the covariant satisfies*

$$\mathbf{D}C_0 = 0 \tag{15}$$

The third type of transformation (12) with determinant $\delta = 1$ when applied to a binary form (7), transforms the coefficients into

$$a'_i = a_i + \binom{n-i}{1} a_{i+1}\nu + \binom{n-i}{2} a_{i+2}\nu^2 + \cdots + a_n\nu^{n-i}.$$

An invariant $\mathcal{I}$ has to satisfy the equation $\mathcal{I}(a'_0, \cdots, a'_n) = \mathcal{I}(a_0, \cdots, a_n)$ for all $\nu$. Hence, differentiating both sides with respect to $\nu$ gives

$$\frac{\partial \mathcal{I}(a')}{\partial a'_0}\frac{da'_0}{d\nu} + \frac{\partial \mathcal{I}(a')}{\partial a'_1}\frac{da'_1}{d\nu} + \cdots + \frac{\partial \mathcal{I}(a')}{\partial a'_n}\frac{da'_n}{d\nu} = 0.$$

We also know that $\frac{da'_i}{d\nu} = (n-i)a'_{i+1}$. The above differential equation becomes

$$na'_1\frac{\partial \mathcal{I}(a')}{\partial a'_0} + (n-1)a'_2\frac{\partial \mathcal{I}(a')}{\partial a'_1} + \cdots + a'_n\frac{\partial \mathcal{I}(a')}{\partial a'_n} = 0.$$

Again, $\mathcal{I}(a')$ depends on $a'$ in the same way as $\mathcal{I}(a)$ depends on $a$. We can remove the primes from the above differential equation:

**Theorem 5.** *Every invariant of a binary form satisfies the differential equation*

$$\Delta\mathcal{I} := na'_1\frac{\partial \mathcal{I}(a')}{\partial a'_0} + (n-1)a'_2\frac{\partial \mathcal{I}(a')}{\partial a'_1} + \cdots + a'_n\frac{\partial \mathcal{I}(a')}{\partial a'_n} = 0. \qquad (16)$$

Similar analysis for covariants gives the following

**Theorem 6.** *Every covariant of a binary form satisfies the differential equation*

$$\Delta\mathcal{C} = x_1\frac{\partial \mathcal{C}}{\partial x_2}. \qquad (17)$$

For invariants, each of the theorems 1, 3 and 5, has a converse. The three converses together form sufficient conditions that characterize invariants for a binary form. However, one might ask whether these conditions are necessary. In fact, the converse of theorem 5 follows from the converses of theorems 1 and 3. Hence, the necessary and sufficient conditions to characterize invariants are as follows

**Theorem 7.** *Every homogeneous isobaric function $\mathcal{I}$ of the coefficients $a_0, a_1, \cdots, a_n$ of degree $g$ and weight $p$, where $ng = 2p$, is an invariant for a binary form if $\mathcal{I}$ satisfies the differential equation $\mathbf{D}\mathcal{I} = 0$.*

In other words, the condition $\Delta\mathcal{I} = 0$ is redundant if the conditions in the above theorem (7) hold.

We ask the same question for covariants. Analogously, theorems 2, 4 and 6 have converses that form sufficient conditions to characterize covariants for binary form. The corresponding necessary conditions are summarized below:

**Theorem 8.** *The function*

$$\mathcal{C} = C_0 x_1^m + \binom{m}{1} C_1 x_1^{m-1} x_2 + \binom{m}{2} C_2 x_1^{m-2} x_2^2 + \cdots + C_m x_2^m$$

*is a covariant of a binary form if and only if $C_0$ is a homogeneous isobaric function in the coefficients $a$, of degree $g$ and weight $p$, such that $m = ng - 2p$, and satisfies the differential equation*

$$\mathbf{D}C_0 = 0.$$

*Also, $C_1, C_2, \cdots, C_m$ are derived from $C_0$ via the formula*

$$C_i = \frac{1}{m(m-1)(m-2)\cdots(m-i+1)} \Delta^i C_0.$$

### 4.2 Simultaneous Invariants and Covariants.

Consider a system of simultaneous binary forms of orders $n, m, \cdots$.

$$\begin{aligned} \mathcal{F}_1 =& a_0 x_1^n + \binom{n}{1} a_1 x_1^{n-1} x_2 + \cdots + a_n x_2^n \\ \mathcal{F}_2 =& b_0 x_1^m + \binom{m}{1} b_1 x_1^{m-1} x_2 + \cdots + b_m x_2^m \\ &\vdots \end{aligned} \tag{18}$$

We apply the same linear transformation to both of them

$$\begin{aligned} x_1 =& \alpha_{11} x_1' + \alpha_{12} x_2' \\ x_2 =& \alpha_{21} x_1' + \alpha_{22} x_2' \end{aligned}$$

where the determinant is $\delta = \alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21}$. This transformation yiels a corresponding system of simultaneous transformed forms. We ask the same question: what kind of functionchanges only by some power of $\delta$ under the transformation? We define simultaneous invariant and covariant as

**Definition 9.** *A simultaneous invariant of the system of forms (18) is a homogeneous polynomial $\mathcal{I}$ of the coefficients $a, b, \cdots$ that satisfies the condition*

$$\mathcal{I}(a'_0, a'_1, \cdots, a'_n; b'_0, b'_1, \cdots, b'_m; \cdots) = \delta^p \mathcal{I}(a_0, a_1, \cdots, a_n; b_0, b_1, \cdots b_m; \cdots) \tag{19}$$

*where $p$ is the weight of the invariant.*

**Definition 10.** *A simultaneous covariant of the forms (18) is a polynomial $\mathcal{C}$ homogeneous in coefficients $a, b, \cdots$ and homogeneous in variables $x$, satisfying the condition*

$$\mathcal{C}(a'_0, a'_1, \cdots, a'_n; b'_0, b'_1, \cdots, b'_m; \cdots; x'_1, x'_2) = \delta^p \mathcal{C}(a_0, a_1, \cdots, a_n; b_0, b_1, \cdots b_m; \cdots; x_1, x_2) \tag{20}$$

*where $p$ is the weight of the covariant.*

By decomposing linear transformation into the three basic type of linear transformations (10), (11) and (12, and applying each transformation to the system of forms (18), we can arrive at the invariant property as before.

Define

$$\begin{aligned}
\mathbf{D}_a =& a_0 \frac{\partial}{\partial a_1} + 2a_1 \frac{\partial}{\partial a_2} + \cdots + n a_{n-1} \frac{\partial}{\partial a_n} \\
\mathbf{D}_b =& b_0 \frac{\partial}{\partial b_1} + 2b_1 \frac{\partial}{\partial b_2} + \cdots + m b_{m-1} \frac{\partial}{\partial b_m} \\
& \vdots \\
\mathbf{D} =& \mathbf{D}_a + \mathbf{D}_b + \cdots \\
\Delta_a =& n a_1 \frac{\partial}{\partial a_0} + (n-1) a_2 \frac{\partial}{\partial a_1} + \cdots + a_n \frac{\partial}{\partial a_{n-1}} \\
\Delta_b =& m b_1 \frac{\partial}{\partial b_0} + (m-1) b_2 \frac{\partial}{\partial b_1} + \cdots + b_m \frac{\partial}{\partial b_{m-1}} \\
& \vdots \\
\Delta =& \Delta_a + \Delta_b + \cdots
\end{aligned}$$

We summarize the neccessary and sufficient conditions

**Theorem 9.** *Suppose $C_0$ is a homogeneous polynomial in coefficients $a_i$ of base form $\mathcal{F}_1$ of degree $n$, coefficients $b_i$ of base form $\mathcal{F}_2$ of degree $m$, etc.; is isobaric in all coefficient sequences, of total weight $p$; and satisfies*

$$\mathbf{D} C_0 = 0.$$

*Then, there is a unique covariant with source $C_0$, i.e.*

$$\mathcal{C} = C_0 x_1^M + \frac{1}{1!}\Delta C_0 x_1^{M-1} x_2 + \frac{1}{2!}\Delta^2 C_0 x_1^{M-2} x_2^2 + \cdots + \frac{1}{M!}\Delta^M C_0 x_2^M.$$

*This simultaneous covariant of forms $\mathcal{F}_1, \mathcal{F}_2, \cdots$ is of degree $r$ in $a_i$, of degree $s$ in $b_i, \cdots$, is homogeneous, and has weight $p$ and order $M = nr + ms + \cdots - 2p$.*
*When $M = 0$, these conditions are sufficient and necessary for a simultaneous invariant.*

Covariants and invariants are very intimately connected. In fact, the following theorem discusses this connection:

**Theorem 10.** *A covariant of a system of forms that is homogeneous in $x_1, x_2$ and of weight $p$ and order $M$ can be transformed into a simultaneous invariant of weight $p + M$ of those base forms together with the linear form $b_0 x_1 + b_1 x_2$, if $x_1$ is replaced by $-b_1$ and $x_2$ by $b_0$.*

To see this, consider the linear transformation again:

$$\begin{aligned} x_1 =& \alpha_{11} x_1' + \alpha_{12} x_2', \\ x_2 =& \alpha_{21} x_1' + \alpha_{22} x_2'; \end{aligned}$$

Inverting these variables gives

$$\begin{aligned} \delta x_1' =& \alpha_{22} x_1 - \alpha_{12} x_2, \\ \delta x_2' =& -\alpha_{21} x_1 + \alpha_{11} x_2. \end{aligned} \tag{21}$$

The linear form is then transformed into

$$\begin{aligned} b_0' x_1' + b_1' x_2' =& b_0 x_1 + b_1 x_2 \\ =& b_0(\alpha_{11} x_1' + \alpha_{12} x_2') + b_1(\alpha_{21} x_1' + \alpha_{22} x_2') \\ =& (b_0\alpha_{11} + b_1\alpha_{21}) x_1' + (b_0\alpha_{12} + b_1\alpha_{22}) x_2' \\ \Rightarrow b_0' =& b_0\alpha_{11} + b_1\alpha_{21}, \\ b_1' =& b_0\alpha_{12} + b_1\alpha_{22}. \end{aligned}$$

Solving for $b_0, b_1$, we get

$$\begin{aligned} -b_1 =& \frac{1}{\delta}(-\alpha_{11} b_1' + \alpha_{12} b_0') \\ b_0 =& \frac{1}{\delta}(-\alpha_{21} b_1' + \alpha_{22} b_0') \end{aligned} \tag{22}$$

Hence, modulo factor $\frac{1}{\delta}$, equations (21) and (22) show that $x_1, x_2$ can be expressed in terms of $x_1', x_2'$ in the same way as $-b_1, b_0$ can be expressed in terms of $-b_1', b_0'$.

Now, for a covariant $\mathcal{C}$,

$$\mathcal{C}(\cdots; x_1', x_2') = \delta^p \mathcal{C}(\cdots; x_1, x_2).$$

Substituting $-b_1$ for $x_1$, $b_0$ for $x_2$, $-\frac{b_1'}{\delta}$ for $x_1'$ and $\frac{b_0'}{\delta}$ for $x_2'$, we get

$$\begin{aligned}
\mathcal{C}\left(\cdots; -\frac{b_1'}{\delta}, \frac{b_0'}{\delta}\right) =& \delta^p \mathcal{C}(\cdots; -b_1, b_0), \\
\frac{1}{\delta^M}\mathcal{C}(\cdots; -b_1' b_0') =& \delta^p \mathcal{C}(\cdots; -b_1, b_0) \\
\mathcal{C}(\cdots; -b_1', b_0') =& \delta^{p+M} \mathcal{C}(\cdots; -b_1, b_0)
\end{aligned}$$

since $\mathcal{C}$ is homogeneous in the variables with order $M$.

This is consistent with the differential operators $\mathbf{D}$ and $\Delta$. $\mathcal{C}$ is a covariant with coefficients $a$ and variables $x_1, x_2$ implies $\mathbf{D}_a \mathcal{C} = x_2 \frac{\partial \mathcal{C}}{\partial x_1}$. Substituting $x_1$ by $-b_1$ and $x_2$ by $b_0$, we have $\mathbf{D}_a \mathcal{C} + b_0 \frac{\partial \mathcal{C}}{\partial b_1} = 0 \Rightarrow \mathbf{D}\mathcal{C} = 0$, which is a defining property for invariant. The idea for $\Delta$ is similar.

Hence, when the number of base forms are not specified, we only need to consider invariants.

## 4.3 Generating Invariants and Covariants

We shall discuss two general methods of generating invariants and covariants – the $p$-th *transvection* and the $\Omega$ process.

### 4.3.1 The $p$-th Transvection

Let $f$ be a base form of order $n$ and $g$ be another base form of order $m$, $n \geq m$. There there is one and only one simultaneous covariant of $f$ and $g$ that is homogeneous and linear in the coefficients of both forms, with weight $p \leq m$, i.e.

$$(f, g)_p = \mathcal{C} = \left( \sum_{i=0}^{p} (-1)^i a_i b_{p-i} \binom{p}{i} \right) x_1^{n+m-2p} + \cdots, \quad p \leq m. \tag{23}$$

This is the $p$-th transvection of $f$ over $g$.

Note that the $p$-th transvection of $g$ over $f$ can differ from that of $f$ over $g$ at most by a sign.

**Example 8.** *The first transvection of $f$ over $g$*

$$(f,g)_1 = (a_0b_1 - a_1b_0)x_1^{n+m-2} + \cdots$$

*is called the functional determinant or Jacobian covariant of the two forms. It can be written as*

$$\begin{vmatrix} \frac{\partial f}{\partial x_1} & \frac{\partial f}{\partial x_2} \\ \frac{\partial g}{\partial x_1} & \frac{\partial g}{\partial x_2} \end{vmatrix}$$

*up to a constant factor.*

The transvection process is a fundamental process to construct covariants. For a system of base forms, if we form all possible transvections and transvections of transvections and base forms, and continues in this fashion, then we obtain all existing covariants [5].

More importantly, we have the following result:

**Theorem 11.** *Every simultaneous covariant $\mathcal{C}$ of base forms $f$ and $g$ of orders $n$ and $m$ respectively, $m \leq n$, can be expressed as*

$$\mathcal{C} = \frac{Poly(f, f_2, \cdots, f_n, g, s_1, s_2, \cdots, s_m)}{f^N} \tag{24}$$

*where $N \in \mathbb{Z}^+$.*

$$f_i = \begin{cases} \frac{1}{2}(f,f)_i & \text{if } i \text{ is even,} \\ (f_{i-1}, f)_1 & \text{if } i \text{ is odd.} \end{cases} \qquad \text{and} \quad s_i = (f,g)_i.$$

### 4.3.2 The $\Omega$ Process

The $\Omega$ process is due to Cayley. Aside from generating covariants, it is an important ingredient in the proof of Hilbert's Finite Basis Theorem which we shall discuss next.

Given a system of binary forms

$$\begin{aligned} \mathcal{F}_1 =& a_0x_1^n + \binom{n}{1}a_1x_1^{n-1}x_2 + \cdots + a_nx_2^n \\ \mathcal{F}_2 =& b_0x_1^m + \binom{m}{1}b_1x_1^{m-1}x_2 + \cdots + b_mx_2^m \\ \vdots & \end{aligned}$$

A linear transformation with determinant $\delta = \alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21}$

$$\begin{aligned} x_1 =& \alpha_{11}x_1' + \alpha_{12}x_2' \\ x_2 =& \alpha_{21}x_1' + \alpha_{22}x_2' \end{aligned}$$

yields a system of transformed forms

$$\begin{aligned} \mathcal{F}_1' =& a_0'x_1'^n + \binom{n}{1} a_1'x_1'^{n-1}x_2' + \cdots + a_n'x_2'^n \\ \mathcal{F}_2' =& b_0'x_1'^m + \binom{m}{1} b_1'x_1'^{m-1}x_2' + \cdots + b_m'x_2'^m \\ & \vdots \end{aligned}$$

**Definition 11.** *We define the $\Omega$ operator to be*

$$\Omega = \begin{vmatrix} \frac{\partial}{\partial\alpha_{11}} & \frac{\partial}{\partial\alpha_{12}} \\ \frac{\partial}{\partial\alpha_{21}} & \frac{\partial}{\partial\alpha_{22}} \end{vmatrix} = \frac{\partial^2}{\partial\alpha_{11}\partial\alpha_{22}} - \frac{\partial^2}{\partial\alpha_{12}\partial\alpha_{21}} \tag{25}$$

The following theorem describes the $\Omega$ process:

**Theorem 12.** *Let $f(a', b', \cdots)$ be any polynomial functin of the transformed coefficients $a', b', \cdots$. If the operator $\Omega$ is applied $p$ times to $\delta^\gamma f(a', b', \cdots)$ until $\Omega^p\left(\delta^\gamma f(a', b', \cdots)\right)$ does nto contain $\alpha_{11}, \alpha 12, \alpha_{21}, \alpha_{22}$ anymore, then we obtain an invariant*

$$\mathcal{I}(a, b, \cdots) = \Omega^p\left(\delta^\gamma f(a', b', \cdots)\right)$$

*of weight $p - \gamma$.*

This theorem has the following converse:

**Theorem 13.** *For every invariant $\mathcal{I}$, there exists a function $f$ such that, for suitable $\gamma$ and $p$, the equation*

$$\mathcal{I}(a, b, \cdots) = \Omega^p\left(\delta^\gamma f(a', b', \cdots)\right)$$

*holds.*

In fact, $f = C \cdot \mathcal{I}$ with the constant $C = \frac{1}{\Omega^p\delta^p}$ and $\Omega^p\delta^p = (p+1)p! \neq 0$.

### 4.4 Hilbert's Finite Basis Theorem

First, we shall quote Hilbert's Finite Basis Theorem for ideals:

**Theorem 14.** *Let $f_1, f_2, \cdots$ be an infinite sequence of forms in $n$ variables $x_1, x_2, \cdots, x_n$. Then there exist $m \in \mathbb{N}$ such that every from $f$ in the sequence can be expressed as*

$$f = A_1 f_1 + A_2 f_2 + \cdots + A_m f_m,$$

*where $A_1, A_2, \cdots, A_m$ are suitable forms of the same $n$ variables. In other words, every homogeneous polynomial ideal has a finite basis.*

There is a finite basis theorem for ring of invariants that follows from Hilber't theorem and the $\Omega$ process.

We start with a binary form of order $n$

$$\mathcal{F}(x_1, x_2) = a_0 x_1^n + \binom{n}{1} a_1 x_1^{n-1} x_2 + \cdots + a_n x_2^n.$$

The invariants are forms in the $n+1$ variables $a_0, a_1, \cdots, a_n$. For a given degreee, the number of invariants is finite. Hence, we can order the invariants, e.g. the ordering in division algorithms: $a_0^g; a_0^{g-1} a_1, a_0^{g-1} a_2, \cdots, a_0 g - 1 a_n; a_0^{g-2} a_1^2, a_0^{g-2} a_1 a_2, \cdots$. Suppose, the sequence of invariants is

$$i_1, i_2, i_3, \cdots$$

By Hilbert's Finite Basis Theorem (14), there exists $m \in \mathbb{N}$ such that any invariant $i$ in the sequence can be written as

$$i = A_1 i_1 + A_2 i_2 + \cdots + A_m i_m$$

where $A_1, \cdots A_m$ are forms in the $a$. Now, under any linear transformation, we have

$$i(a') = A_1(a') \cdot i_1(a') + A_2(a') \cdot i_2(a') + \cdots + A_m(a') \cdot i_m(a') \tag{26}$$

where $a'$ are the transformed coefficients of the binary form. Since $i, i_1, i_2, \cdots, i_m$ are invariants with weights $\gamma, \gamma_1, \gamma_2, \cdots, \gamma_m$, equation (26) becomes

$$\delta^\gamma i(a) = A_1(a') \cdot \delta^{\gamma_1} i_1(a) + A_2(a') \cdot \delta^{\gamma_2} i_2(a) + \cdots + A_m(a') \cdot \delta^{\gamma_m} i_m(a). \tag{27}$$

Applying the operator $\Omega$ $\gamma$ times to both sides, we arrive at

$$i(a) \Omega^\gamma \delta^\gamma = i_1(a) \Omega^\gamma \left( \delta^{\gamma_1} A_1(a') \right) + \cdots + i_m(a) \Omega^\gamma \left( \delta^{\gamma_m} A_m(a') \right). \tag{28}$$

Since $i_j(a') = \delta^{\gamma_j} i_j(a)$, $\delta^{\gamma_j}$ contains $\alpha_{11}, \alpha_{12}, \alpha_{21}, \alpha_{22}$ to the same degree as $i_j(a')$. Hence, $A_j(a') \cdot \delta^{\gamma_j}$ contains the $\alpha$'s to the same degree as $i_j(a')A_j(a')$, which in turn is the same degree $\alpha$'s appear in $i(a')$, i.e. $\gamma$. Hence, applying $\Omega$ $\gamma$ times will exactly eliminate the $\alpha$'s. Theorem (12) implies that each $\Omega^\gamma$ $(\delta^{\gamma_j} A_j(a'))$ is an invariant.

$$i(a) = \mathcal{I}_1(a) \cdot i_1(a) + \mathcal{I}_2(a) \cdot i_2(a) + \cdots + \mathcal{I}_m(a) i_m(a). \tag{29}$$

Since $i_1(a), i_2(a), \cdots, i_m(a)$ are of degree at least one, $\mathcal{I}_1, \mathcal{I}_2, \cdots, \mathcal{I}_m$ must be lower degree than $i(a)$. We repeat this whole process for each $\mathcal{I}_j$ as we did for $i(a)$ until the degree of the invariants $\mathcal{I}$ is smaler than that of $i_m$. Hence, these $\mathcal{I} \in \{i_1, \cdots, i_m\}$. This proves that every invariant is a polynomial function of the invariants $i_1, i_2, \cdots, i_m$. We summarize this result as follows:

**Theorem 15.** *The invariant ring, i.e. the linear span of all invariants that are homogeneous polynomials, for every binary form has a finite basis. In particular, every invariant of the form is a polynomial function of the invariants in the basis.*

This theorem can be extended to system of base forms.

**Theorem 16.** *For any system of binary forms subject to linear transformation of $x_1, x_2$, the invariant ring has a finite basis. In particular, every simultaneous invariant can be written as a polynomial function of the invariants in the basis.*

This also implies the existence of finite basis for covariants since covariants are equivalent to simultaneous invariants of the same system of base forms plus a linear form.

### 4.5 Hilbert Series

**Definition 12.** *A ring $R$ over a field $k$ is (multi)graded if $R$ can be written as a direct sum*

$$R = \bigoplus_{\mathbf{g} \in (\mathbb{Z}^+)^n} R_{\mathbf{g}}$$

*where each $R_{\mathbf{g}}$ is a $k$-vector space and*

$$R_{\mathbf{g}_1} \cdot R_{\mathbf{g}_2} \subset R_{\mathbf{g}_1 + \mathbf{g}_2}.$$

*The elements of $R_{\mathbf{g}}$ are called homogeneous of (multi)degree $g$. [10, 8]*

**Example 9.** *The multi-graded ring of interest to us is the ring of polynomials* $k[\mathbf{a}, \mathbf{b}, \cdots, \mathbf{w}]$, $\mathbf{a} = a_0, a_1, \cdots, a_{n_1}$, $\mathbf{b} = b_0, b_1, \cdots, b_{n_2}, \cdots$, $\mathbf{w} = w_0, w_1, \cdots, w_{n_k}$. *The multidegree consists of degrees of the homogeneous polynomials in* $\mathbf{a}, \mathbf{b}, \cdots, \mathbf{w}$ *and the weight of the isobaric polynomials. That is, if*

$$f = Ca_0^{\alpha_0} a_1^{\alpha_1} \cdots a_{n_1}^{\alpha_{n_1}} \cdots w_0^{\gamma_0} \cdots w_{n_k}^{\gamma_{n_k}},$$

*then*

$$\text{degree}(f) := \mathbf{g} = (\alpha_0 + \alpha_1 + \cdots + \alpha_{n_1}, \cdots, \gamma_0 + \gamma_1 + \cdots + \gamma_{n_k})$$
$$\text{weight}(f) := p = (\alpha_1 + 2\alpha_2 + 3\alpha_3 + \cdots + n_1\alpha_{n_1}) + \cdots + (\gamma_1 + 2\gamma_2 + \cdots + n_k\gamma_{n_k}).$$

*Hence,* $k[\mathbf{a}, \mathbf{b}, \cdots, \mathbf{w}]$ *is a graded* $(\mathbf{g}, p)$ *ring.*

We introduce the Hilbert series (or Poincare series) for graded rings:

**Definition 13.** *The* Hilbert series *is*

$$H(R, \mathbf{z}) = \sum_{g_k=0}^{\infty} \sum_{g_{k-1}=0}^{\infty} \cdots \sum_{g_1=0}^{\infty} \left(\dim(R_{\mathbf{g}}) z_1^{g_1} \cdots z_k^{g_k}\right) \tag{30}$$

*where* $\mathbf{z} = (z_1, z_2, \cdots, z_k)$ *and* $\dim(R_{\mathbf{g}})$ *is the number of linearly independent invariants of degree* $g_i$ *in the coefficients of the* $i$*-th form, for all* $i = 1, 2, \cdots, k$.

Let's first consider a useful and simple example of Hilbert series. We shall state it as a lemma.

**Lemma 1.** *Suppose* $u_1, u_2, \cdots, u_m$ *are algebraically independent elements of polynomial ring* $k[\mathbf{x}]$*, that are homogeneous of degrees* $\mathbf{g}_1, \mathbf{g}_2, \cdots, \mathbf{g}_m$ *respectively. Then, the Hilbert series of the graded subring* $R := k[u_1, u_2, \cdots, u_m]$ *is*

$$H(R, \mathbf{z}) = \sum_{\mathbf{g}} \dim(R_{\mathbf{g}}) \mathbf{z}^{\mathbf{g}} = \frac{1}{(1 - \mathbf{z}^{\mathbf{g}_1})(1 - \mathbf{z}^{\mathbf{g}_2}) \cdots (1 - \mathbf{z}^{\mathbf{g}_m})} \tag{31}$$

*Proof.* Since $u_j$ are algebraically independent, the set

$$\{u_1^{i_1} u_2^{i_2} \cdots u_m^{i_m} \mid i_1, i_2, \cdots, i_m \in \mathbb{N}, \sum_j i_j \mathbf{g_j} = \mathbf{g}\}$$

is a basis for the vector space $R_{\mathbf{g}}$.

Let

$$A_{\mathbf{g}} := \{(i_1, i_2, \cdots, i_m) \in \mathbb{N}^m \mid \sum_j i_j \mathbf{g_j} = \mathbf{g}\}$$

Then, $\dim(R_{\mathbf{g}}) = \dim(A_{\mathbf{g}})$.

Consider the expansion

$$\begin{aligned}\frac{1}{(1-\mathbf{z}^{\mathbf{g}_1})(1-\mathbf{z}^{\mathbf{g}_2})\cdots(1-\mathbf{z}^{\mathbf{g}_m})} &= \left(\sum_{i_1=0}^{\infty}\mathbf{z}^{i_1\mathbf{g_1}}\right)\left(\sum_{i_2=0}^{\infty}\mathbf{z}^{i_2\mathbf{g_2}}\right)\cdots\left(\sum_{i_m=0}^{\infty}\mathbf{z}^{i_m\mathbf{g_m}}\right)\\ &= \sum_{\mathbf{g}}\sum_{(i_1,\cdots,i_m)\in A_{\mathbf{g}}}\mathbf{z}^{\mathbf{g}}\\ &= \sum_{\mathbf{g}}\dim(A_{\mathbf{g}})\mathbf{z}^{\mathbf{g}}\end{aligned}$$

□

To find the Hilbert series, we will need to know $\dim(R_{\mathbf{g}})$ for any set of degree $\mathbf{g}$. But first, let $V^{\mathbf{g},p}$ denote all homogeneous polynomials in $\mathbf{a}, \mathbf{b}, \cdots$ of weight $p$ and degrees $g_1$ in $\mathbf{a}$, $g_2$ in $\mathbf{b}$, $\cdots$ Hence, if $\mathcal{I}$ is an invariant with $\mathcal{I} \in V^{\mathbf{g},p}$, then $\mathbf{n}\cdot\mathbf{g} = n_1g_1 + n_2g_2 + \cdots + n_kg_k = 2p$ and $\mathbf{D}\mathcal{I} = 0$. Note that

$$\mathbf{D} : V^{\mathbf{g},p} \to V^{\mathbf{g},p-1}$$

and

$$\begin{aligned}\dim(R_{\mathbf{g}}) =& \dim\left(\ker\left(D\left(V^{\mathbf{g},\frac{\mathbf{n}\cdot\mathbf{g}}{2}}\right)\right)\right)\\ =& \dim\left(V^{\mathbf{g},\frac{\mathbf{n}\cdot\mathbf{g}}{2}}\right) - \dim\left(\text{Image}\left(D\left(V^{\mathbf{g},\frac{\mathbf{n}\cdot\mathbf{g}}{2}}\right)\right)\right)\end{aligned}$$

We shall first prove the following proposition that we will need later. The version for polynomials of one variable is described in [6].

**Proposition 1.**

$$\text{Image}(\mathbf{D}(V^{\mathbf{g},p})) = V^{\mathbf{g},p-1} \tag{32}$$

*if* $2p = \mathbf{n}\cdot\mathbf{g}$.

*Proof.* $\text{Image}(\mathbf{D}(V^{\mathbf{g},p})) \subseteq V^{\mathbf{g},p-1}$ is obvious. Also, $\Delta : V^{\mathbf{g},p-1} \to V^{\mathbf{g},p}$. Hence, $\text{Image}(\mathbf{D}\circ\Delta(V^{\mathbf{g},p})) \subseteq \text{Image}(D(V^{\mathbf{g},p})) \subseteq V^{\mathbf{g},p-1}$.

Now, suppose $\dim(V^{\mathbf{g},p-1}) - \dim(\text{Image}(\mathbf{D}\circ\Delta(V^{\mathbf{g},p}))) > 0$. That is $\dim(\ker(\mathbf{D}\circ\Delta(V^{\mathbf{g},p}))) > 0$. Hence, there exists $\mathcal{K} \neq 0$, $\mathcal{K} \in \ker(\mathbf{D}\circ\Delta(V^{\mathbf{g},p}))$, i.e $\mathbf{D}(\Delta\mathcal{K}) = 0$.

Consider $l \in \mathbb{N}$ such that $\mathbf{D}^l\mathcal{K} = 0$ but $\mathbf{D}^{l-1}\mathcal{K} \neq 0$. There is such a $l$ since $\mathbf{D}$ reduces the weight of $\mathcal{K}$ by 1 per application and the weight has to exhaust when $\mathbf{D}$ is applied enough time. Also $l > 0$ since $\mathcal{K} = 0$ otherwise.

Note that $\mathbf{D}$ and $\Delta$ has a commutator relation

$$\mathbf{D}^k\Delta - \Delta\mathbf{D}^k = k(\mathbf{n}\cdot\mathbf{g} - 2p + k - 1)\mathbf{D}^{k-1} \tag{33}$$

when acting on a polynomial of degree $\mathbf{g}$ and weight $p$. Hence,

$$(\mathbf{D}^l\Delta - \Delta\mathbf{D}^l)\mathcal{K} = l(\mathbf{n}\cdot\mathbf{g} - 2p + l + 1)\mathbf{D}^{l-1}\mathcal{K}$$

The left hand side of the equation is 0 since $\mathbf{D}\Delta\mathcal{K} = 0$ and $\mathbf{D}^l\mathcal{K} = 0$. On the right hand side, $\mathbf{D}^{l-1}\mathcal{K} \neq 0$ and $l \neq 0$ as discussed above. Also, by assumption $\mathbf{n}\cdot\mathbf{g} = 2p$. This implies $l = -1$ which is a contradiction.

Hence, $\dim(V^{\mathbf{g},p-1}) - \dim(\mathrm{Image}(\mathbf{D}\circ\Delta(V^{\mathbf{g},p}))) = 0 \Rightarrow V^{\mathbf{g},p-1} = \mathrm{Image}(\mathbf{D}\circ\Delta(V^{\mathbf{g},p})) \Rightarrow \mathrm{Image}(\mathbf{D}(V^{\mathbf{g},p})) = V^{\mathbf{g},p-1}$. □

This proposition gives

$$\dim(R_{\mathbf{g}}) = \dim\left(V^{\mathbf{g},\frac{\mathbf{n}\cdot\mathbf{g}}{2}}\right) - \dim\left(V^{\mathbf{g},\frac{\mathbf{n}\cdot\mathbf{g}}{2}-1}\right) \tag{34}$$

To compute $\dim(R_{\mathbf{g}})$, we need to be able to find $\dim(V^{\mathbf{g},p})$. Although invariants always satisfy $\mathbf{n}\cdot\mathbf{g} = 2p$, it will be useful to first treat $p$ as independent and impose the condition later. Hence, we need to consider the weight $p$ as an extra grading and derive the *bi-graded* Hilbert series, graded both by weight and degree. We shall start with one binary form.

**Proposition 2.** *Let* $\mathcal{F} = a_0x_1^n + \binom{n}{1}x_1^{n-1}x_2 + \cdots + a_nx_2^n$ *be a binary of order* $n$. *If* $C_{g,p} = \dim(V^{g,p})$, *then*

$$\frac{1}{(1-zt_1^n)(1-zt_1^{n-1}t_2)(1-zt_1^{n-2}t_2^2)\cdots(1-zt_2^n)} = \sum_g\sum_{p=0}^{ng} C_{g,p}z^g t_1^{ng-p}t_2^p.$$

*Proof.* This is just a calculation. Consider expanding the series

$$\begin{aligned}
\frac{1}{1-zt_1^n} =& 1 + zt_1^n + z^2t_1^{2n} + \cdots \\
=& \sum_{\nu_0=0}^{\infty} z^{\nu_0} t_1^{n\nu_0} \\
\frac{1}{1-zt_1^{n-1}t_2} =& 1 + zt_1^{n-1}t_2 + z^2t_1^{2(n-1)}t_2^2 + \cdots \\
=& \sum_{\nu_1=0}^{\infty} z^{\nu_1} t_1^{(n-1)\nu_1} t_2^{\nu_1} \\
& \vdots \\
\frac{1}{1-zt_2^n} =& \sum_{\nu_n=0}^{\infty} z^{\nu_n} t_2^{n(\nu_n)} \\
\Rightarrow \prod_{j=0}^{n} \frac{1}{(1-zt_1^{n-j}t_2^j)} =& \sum_{\nu_0,\nu_1,\cdots} z^{\nu_0+\nu_1+\cdots+\nu_n} t_1^{n\nu_0+(n-1)\nu_1+\cdots+\nu_{n-1}} t_2^{\nu_1+2\nu_2+\cdots+n\nu_n} \\
=& \sum_{g,p} C_{g,p} z^g t_1^{ng-p} g_2^p
\end{aligned}$$

□

**Remark 1.** *The formula in the proposition above can be translated as a hilbert series since*

$$\begin{aligned}
\prod_{j=0}^{n} \frac{1}{(1-zt_1^{n-j}t_2^j)} =& \sum_{g,p} C_{g,p} z^g t_1^{ng-p} g_2^p \\
=& \sum_{g,p} C_{g,p} (zt_1^n)^g \left(\frac{t_2}{t_1}\right)^p \\
=& H\left(k[a_0, a_1, \cdots, a_n], zt_1^n, \frac{t_2}{t_1}\right)
\end{aligned}$$

*which is a bi-graded Hilbert series over the polynomial ring $k[a_0, \cdots, a_n]$, graded by degree (represented by variable $zt_1^n$) and weight (represented by variable $\frac{t_2}{t_1}$).*

We shall extend proposition (2) to system of many forms. Note that the coefficients of the forms are independent. Hence, the power series associated

to each form, i.e. as in proposition (2), can be multiplied in very much the same way as in the proof of proposition (2). We describe the extension as follows:

**Proposition 3.** *Given a system of $k$ base forms $\mathcal{F}_1, \cdots, \mathcal{F}_k$ with order $n_1, n_2, \cdots, n_k$,*

$$P(\mathbf{z}, t_1, t_2) = \sum_{\mathbf{g}} \sum_{p=0}^{\mathbf{n}\cdot\mathbf{g}} C_{\mathbf{g},p} z^{\mathbf{g}} t_1^{\mathbf{n}\cdot\mathbf{g}-p} t_2^p = \prod_{i=1}^{k} \prod_{j=0}^{n_i} \frac{1}{1 - z_i t_1^{n_i - j} t_2^j}$$

*where $\mathbf{z} = (z_1, z_2, \cdots, z_k)$, $z_i$ is the dummy variable corresponds to the $i$-th form, and, $\mathbf{g} = (g_1, g_2, \cdots, g_k)$,$g_i$ is the degree of coefficients of $i$-th form.*

Now, we are in position to calculate $\dim(R_{\mathbf{g}})$.

**Proposition 4.** *Recall that*

$$\dim(R_{\mathbf{g}}) = C_{\mathbf{g},p} - C_{\mathbf{g},p-1}$$

*with $p = \frac{\mathbf{n}\cdot\mathbf{g}}{2}$.*

*Then, $\dim(R_{\mathbf{g}})$ is the coefficient of $\mathbf{z}^{\mathbf{g}}(t_1 t_2)^{p+1}$ in the power series generated by*

$$\frac{t_1 t_2 - t_2^2}{\prod_{i=1}^{k} \prod_{j=0}^{n_i} (1 - z_i t_1^{n_i - j} t_2^j)}. \tag{35}$$

*Proof.* Recall

$$P(\mathbf{z}, t_1, t_2) = \sum_{\mathbf{g}} \sum_{p=0}^{\mathbf{n}\cdot\mathbf{g}} C_{\mathbf{g},p} z^{\mathbf{g}} t_1^{\mathbf{n}\cdot\mathbf{g}-p} t_2^p.$$

Then, the generating function (35) is

$$(t_1 t_2 - t_2^2) P(\mathbf{z}, t_1, t_2) = \sum_{\mathbf{g}} \sum_{p=0}^{\mathbf{n}\cdot\mathbf{g}} C_{\mathbf{g},p} z^{\mathbf{g}} t_1^{\mathbf{n}\cdot\mathbf{g}-p+1} t_2^{p+1} - \sum_{\mathbf{g}} \sum_{p=0}^{\mathbf{n}\cdot\mathbf{g}} C_{\mathbf{g},p} z^{\mathbf{g}} t_1^{\mathbf{n}\cdot\mathbf{g}-p} t_2^{p+2}$$

In the second sum, we make a change of variable $p' = p + 1$ and then dropping the prime. Also, note that $C_{\mathbf{g},p-1} = 0$ when $p = 0$. Then, we rewrite the expression as

$$(t_1 t_2 - t_2^2) P(\mathbf{z}, t_1, t_2) = \sum_{\mathbf{g}} \sum_{p=0}^{\mathbf{n}\cdot\mathbf{g}} (C_{\mathbf{g},p} - C_{\mathbf{g},p-1}) z^{\mathbf{g}} t_1^{\mathbf{n}\cdot\mathbf{g}-p+1} t_2^{p+1}.$$

Setting $\mathbf{n} \cdot \mathbf{g} = 2p$ yields the result. □

This proposition suggests the following algorithm for computing the Hilbert series for the invariant ring:

**Theorem 17.** *(Algorithm for Computing Hilbert Series)*

1. *Compute* $(t_1 t_2 - t_2^2) P(\mathbf{z}, t_1, t_2)$.
2. *Let* $t_1 t_2 \to 1$. *The remaining dependence in* $t_1$ *and* $t_2$ *in every term cannot be of equal power in* $t_1$ *and* $t_2$.
3. *Set* $t_1 \to 0$ *and* $t_2 \to 0$. *This extracts the terms constant in* $t_1$ *and* $t_2$. *This is the Hilbert series* $H(R, \mathbf{z})$.

## 4.6 Noether Normalization

Much of this material can be found in [9].

First, we need to establish some elementary algebraic ideas.

**Definition 14.** *Let* $A$ *be a ring. An* $A$*-module is an abelian group* $M$ *with a multiplication map* $A \times M \to M$, *i.e.* $(a, m) \to am$ *such that for any* $a, b \in A$, $m, n \in M$,

$$\begin{aligned} a(m+n) &= am + an \\ (a+b)m &= am + bm \\ (ab)m &= a(bm) \\ 1_A m &= m \end{aligned}$$

*A subset* $N \subset M$ *is a submodule if* $am + bn \in N$ *for all* $a, b \in A$, $m, n \in N$. *A homomorphism* $\phi : M \to N$ *is an* $A$*-linear map on* $A$*-modules if* $\phi(am + bn) = a\phi(m) + b\phi(n)$ *for* $a, b \in A$, $m, n \in M$.

Note that A module over a field $k$ is a vector space over $k$.

**Definition 15.** *A module* $M$ *is said to be finitely generated if there exists* $m_1, m_2, \cdots, m_r \in M$ *such that* $M =< m_1, m_2, \cdots, m_r >$ . *Furthermore, if* $m_1, m_2, \cdots, m_r$ *form a basis for* $M$, *then,* $M$ *is a* free *module.*

**Example 10.** *Let* $M \subset \mathbb{C}[x, y]$ *consisting of polynomials of the form*

$$P = x^3\, p_1(x, y) + (xy)\, p_2(x, y) + y^3\, p_3(x, y).$$

*Then,* $M$ *is a* $\mathbb{C}[x, y]$ *module generated by* $x^3, xy, y^3$. $M$ *is also the ideal generated by* $x^3, xy, y^3$. *This set of generators is also an irreducible Groebner*

*basis for the ideal. However, it is not a* linear vector space basis *for $M$ since $P$ has no unique decomposition. For example, $P = x^3y^3$. We can have $(p_1, p_2, p_3)$ to be $(y^3, 0, 0)$ or $(0, x^2y^2, 0)$ or $(0, 0, x^3)$ etc. Hence, $M$ is not a free module.*

**Definition 16.** *A subring $A \subset k[x_1, x_2, \cdots, x_n]$ is finitely generated if there exists $u_1, u_2, \cdots, u_m \in A$ such that $A = k[u_1, u_2, \cdots, u_m]$.*

Note that the set $u_1, u_2, \cdots, u_m$ need not be *algebraically independent.*

**Definition 17.** *A set $u_1, u_2, \cdots, u_m$, $u_i = u_i(\mathbf{x})$, is algebraically independent if the map*

$$k[y_1, y_2, \cdots y_m] \to k[u_1, u_2, \cdots, u_m]$$

*with $y_i \to u_i$ an isomorphism. $k[y_1, y_2, \cdots, y_m]$ is the ring of polynomial of $m$ variables.*

This means a polynomial $P(u_1, u_2, \cdots, u_m)$ is identically zero if and only if $P$ is a zero polynomial. In other words, there is no syzygy among the $u$'s.

Now, we shall describe the Noether normalization – the fundamental property of all finitely generated algebras.

**Lemma 2.** *(Noether normalization)*
*Let $A = k[u_1, u_2, \cdots, u_m]$ be a finitely generated algebra (subring). Then, there exists a finite, algebraically independent set $\theta_1, \theta_2, \cdots, \theta_k \in A$ such that $A$ is a finitely generated module over $B = k[\theta_1, \cdots, \theta_k]$.*

*That is to say, there exists $\eta_1, \eta_2, \cdots, \eta_s \in A$ such that every $P \in A$ can be written as a linear combination:*

$$P = p_1(\theta_1, \theta_2, \cdots, \theta_k)\eta_1 + p_2(\theta_1, \theta_2, \cdots, \theta_k)\eta_2 + \cdots p_s(\theta_1, \cdots, \theta_k)\eta_s.$$

The maximum number of algebraically independent members of $A$ is the *Krull dimension* of $A$.

The Noether normalization admits the special case – Cohen-Macaulay rings.

**Definition 18.** *$A$ is Cohen-Macaulay if the elements $\eta_1, \eta_2, \cdots, \eta_s$ form a basis for $A$ over $B = k[\theta_1, \theta_2, \cdots, \theta_k]$, where $\theta_1, \theta_2, \cdots, \theta_k$ are algebraically independent. That is, every $P \in A$ can be written* uniquely *as a linear combination*

$$P = \sum \eta_i p_i(\theta_1, \theta_2, \cdots, \theta_k).$$

This implies that if $A$ is Cohen-Macaulay, then $\sum_{i=1}^{s} \eta_i p_i = 0 \Rightarrow p_i = 0 \forall i = 1, 2, \cdots, s$. Hence, $A$ is a free module over $B$. In other words, $\eta_i$ are linearly independent over $\theta_j$.

If $A$ is an invariant ring, $\theta_1, \theta_2, \cdots, \theta_k$ are called the *primary invariants* and $\eta_1, \eta_2, \cdots, \eta_s$ are the *secondary invariants*. Hence, we have the following corollary:

**Corollary 1.** *(Hironaka Decomposition)*
*The invariant ring $A$ can be written as*

$$A = \eta_1 k[\theta_1, \cdots, \theta_k] \oplus \eta_2 k[\theta_1, \cdots, \theta_k] \oplus \cdots \oplus \eta_s k[\theta_1, \cdots, \theta_k]. \tag{36}$$

*This is called a* Hironaka decomposition *of $A$.*

We have an immediate extension of lemma 1 for Cohen-Macaulay rings

**Corollary 2.** *A Cohen-Macaulay ring*

$$A = \eta_1 k[\theta_1, \cdots, \theta_k] \oplus \eta_2 k[\theta_1, \cdots, \theta_k] \oplus \cdots \oplus \eta_s k[z-1, \cdots, \theta_k]$$

*where the primary invariants $\theta_i$ are homogeneous of degree $\mathbf{g}_i$ and the secondary invariants $\eta_j$ are homogeneous of degree $\mathbf{g}'_j$, has a Hilbert series*

$$H(R, \mathbf{z}) = \sum_{\mathbf{g}} \dim(R_{\mathbf{g}}) \mathbf{z}^{\mathbf{g}} = \frac{\mathbf{z}^{\mathbf{g}'_1} + \mathbf{z}^{\mathbf{g}'_2} + \cdots + \mathbf{z}^{\mathbf{g}'_k}}{(1 - \mathbf{z}^{\mathbf{g}_1})(1 - \mathbf{z}^{\mathbf{g}_2}) \cdots (1 - \mathbf{z}^{\mathbf{g}_m})} \tag{37}$$

The following theorem sums it up:

**Theorem 18.** *(Hochster & Roberts [7]) The invariant ring for binary forms are Cohen-Macaulay and admit a Hironaka decomposition.*

### 4.7 Computing Hilbert Series for Simultaneous Invariants

In this section, we demonstrate a convenient way to find Hilbert series for a system of forms, using complex integration.

Suppose we are given a system of binary forms

$$\begin{aligned}
\mathcal{F}_1 =& a_0 x_1^{n_1} + \binom{n_1}{1} a_1 x_1^{n_1 - 1} x_2 + \cdots + a_{n_1} x_2^{n_1} \\
\mathcal{F}_2 =& b_0 x_1^{n_2} + \binom{n_2}{1} b_1 x_1^{n_2 - 1} x_2 + \cdots + b_{n_2} x_2^{n_2} \\
& \vdots \\
\mathcal{F}_k =& w_0 x_1^{n_k} + \binom{n_k}{1} w_1 x_1^{n_k - 1} x_2 + \cdots + w_{n_k} x_2^{n_k}
\end{aligned} \tag{38}$$

The Hilbert series for the ring of simultaneous invariants $R$, is given by

$$\begin{aligned} H(R,\mathbf{z}) =& \sum_{\mathbf{g}} \dim(R_{\mathbf{g}})\mathbf{z}^{\mathbf{g}} \\ =& \left( \frac{t_1 t_2 - t_2^2}{\prod_{i=1}^{k} \prod_{j=0}^{n_i} (1 - z_i t_1^{n_i - j} t_2^j)} \right) /.\{t_1 t_2 \to 1\} /.\{t_1 \to 0, t_2 \to 0\} \end{aligned}$$

where the last equation condense the algorithm in Theorem (17). "/." denotes "subject to the condition of" followed by the conditions given in the set notation $\{\cdot\}$.

We first prove the following convergence result

**Lemma 3.** *The series* $\sum \dim(R_{\mathbf{g}})\mathbf{z}^{\mathbf{g}}$ *converges if* $\max_i |z_i| < 1$.

*Proof.* Recall that $V^{\mathbf{g},p}$ is the set of polynomials with degree $\mathbf{g}$ and weight $p$; whereas $R_{\mathbf{g}}$ is the set of polynomial invariants with degree $\mathbf{g}$, i.e. the condition $\mathbf{n} \cdot \mathbf{g} = 2p$ is satisfied. Clearly,

$$\dim(R_{\mathbf{g}}) \leq \dim(V^{\mathbf{g},p}) \leq \sum_{p} \dim(V^{\mathbf{g},p}).$$

However, $\cup_{\mathbf{g},p} V^{\mathbf{g},p} = k[\mathbf{a}, \mathbf{b}, \cdots, \mathbf{w}]$ where $\mathbf{a} = a_1, a_2, \cdots, a_{n_1}; \mathbf{b} = b_1, b_2, \cdots, b_{n_2}; \cdots; \mathbf{w} = w_1, \cdots w_{n_k}$ are all independent since they are coefficients of the given forms as in (38). Each of the $a_i$ or $b_i$ etc. has degree 1. By lemma (1), we have

$$\sum_{\mathbf{g}} \sum_{p} \dim(V^{\mathbf{g},p})\mathbf{z}^{\mathbf{g}} = \frac{1}{\prod_{i=1}^{k} (1 - z_i)^{n_i + 1}}$$

which converges if $\max_i |z_i| < 1$.

Hence, by comparison test, the Hilbert series $\sum_{\mathbf{g}} \dim(R_{\mathbf{g}})\mathbf{z}^{\mathbf{g}}$ converges also when $\max_i |z_i| < 1$. □

The next lemma shows how we can compute Hilbert series by complex integration:

**Lemma 4.** *If* $\max_i |z_i| < 1$, *then,*

$$\begin{aligned} H(R,\mathbf{z}) =& \left( \frac{t_1 t_2 - t_2^2}{\prod_{l=1}^{k} \prod_{j=0}^{n_l} (1 - z_l t_1^{n_l - j} t_2^j)} \right) /.\{t_1 t_2 \to 1\} /.\{t_1 \to 0, t_2 \to 0\} \\ =& \frac{1}{2\pi i} \oint \frac{1 - \tau^2}{\prod_{l=1}^{k} \prod_{j=0}^{n_l} (1 - z_l \tau^{2j - n_l})} \frac{d\tau}{\tau}. \end{aligned} \tag{39}$$

*where the integral is taken over the unit circle.*

*Proof.* For $\max_i |z_i| < 1$, lemma (3) implies we have a formal expansion

$$\frac{t_1 t_2 - t_2^2}{\prod_{l=1}^{k} \prod_{j=0}^{n_l} (1 - z_l t_1^{n_l - j} t_2^j)} = \sum_{\alpha,\beta} P_{\alpha,\beta}(\mathbf{z}) t_1^\alpha t_2^\beta.$$

By algorithm in theorem (17), we need to pick out terms that are equal power in $t_1$ and $t_2$. By moding out factors of $t_1 t_2$ from these terms, we will get the Hilbert series. That is, we need

$$H(R, \mathbf{z}) = \sum_{\alpha} P_{\alpha,\alpha}(\mathbf{z}).$$

Let $t_1 = \frac{1}{\tau}$, $t_2 = \tau$ with $|\tau| = 1$, in the formal expansion above. When $\max_i |z_i| < 1$, we have the convergent series

$$\frac{1 - \tau^2}{\prod_{l=1}^{k} \prod_{j=0}^{n_l} (1 - z_l \tau^{2j - n_l})} = \sum_{\alpha,\beta} P_{\alpha,\beta}(\mathbf{z}) \tau^{\beta - \alpha}.$$

Integrating with respect to $\frac{d\tau}{\tau}$ over the unit circle, we get

$$\frac{1}{2\pi i} \oint \frac{1 - \tau^2}{\prod_{l=1}^{k} \prod_{j=0}^{n_l} (1 - z_l \tau^{2j - n_l})} \frac{d\tau}{\tau} = \sum_{\alpha} P_{\alpha,\alpha}(\mathbf{z}) = H(R, \mathbf{z}).$$

□

Hence, we can calculate the multigraded Hilbert series $H(R, \mathbf{z})$ using the residue theorem.

Consider the integrand

$$\begin{aligned} P(\mathbf{z}, \tau) =& \frac{1 - \tau^2}{\tau \prod_{l=1}^{k} \prod_{j=0}^{n_l} (1 - z_l \tau^{2j - n_l})} \\ =& \frac{(1 - \tau^2) \tau^{-1} \prod_{l=1}^{k} \prod_{j=0}^{\left[\frac{n_l - 1}{2}\right]} \tau^{n_l - 2j}}{\prod_{l=1}^{k} \left( \prod_{j=0}^{\left[\frac{n_l - 1}{2}\right]} (\tau^{n_l - 2j} - z_l) \prod_{j=\left[\frac{n_l + 1}{2}\right]}^{n_l} (1 - z_l \tau^{2j - n_l}) \right)} \end{aligned} \tag{40}$$

The poles that lies inside the unit circle are therefore given by

$$\tau_{l,j,q} = z_l^{\frac{1}{2j - n_l}} \omega^q, \ l = 1, 2, \cdots, k; \ j = \left[\frac{n_l + 1}{2}\right], \cdots, n_l; \ \omega = e^{\frac{2\pi i}{2j - n_l}}.$$

From this, we arrive at the following useful formulation

$$H(R, \mathbf{z}) = \sum_{l=1}^{k} \sum_{j=\left[\frac{n_l + 1}{2}\right]}^{n_l} \sum_{q=1}^{2j - n_l} \operatorname{Res} \left( \frac{1 - \tau^2}{\tau \prod_{l=1}^{k} \prod_{j=0}^{n_l} (1 - z_l \tau^{2j - n_l})}, \tau_{l,j,q} \right) \tag{41}$$

### 4.8 An Extended Example

Here, we shall present an example of using the Hilbert series to compute a Hironaka decomposition of an invariant ring. This example can also be found in [6, 11], where it is treated in a similar but slightly different manner.

Consider the system of forms

$$\begin{aligned}\mathcal{F} =& a_0x_1^3 + 3a_1x_1^2x_2 + 3a_2x_1x_2^2 + a_3x_2^3\\ l =& b_0x_1 + b_1x_2\end{aligned} \tag{42}$$

Let $R$ be the invariant ring generated by the simultaneous invariants of this system of forms. By theorem 18, $R$ is Cohen-Macaulay and has a Hironaka decomposition. In other words, there exists a set of algebraically independent primary invariants $\theta_1, \theta_2, \cdots, \theta_k$ and a set of secondary invariants $\eta_1, \cdots, \eta_s$ that are linearly independent from the primary ones, such that any $f \in R$ can be written as

$$f = \eta_1 P_1(\theta_1, \cdots, \theta_k) + \eta_2 P_2(\theta_1, \cdots, \theta_k) + \cdots + \eta_s P_s(\theta_1, \cdots, \theta_k).$$

To find out what $k, s$ are, we shall compute the Hilbert series. By equation (40), we have in this case,

$$P(z, \zeta, \tau) = \frac{1 - \tau^2}{\tau\left(1 - \frac{z}{\tau^3}\right)\left(1 - \frac{z}{\tau}\right)(1 - z\tau)(1 - z\tau^3)\left(1 - \frac{\zeta}{\tau}\right)(1 - \zeta\tau)}.$$

Hence, the only poles in the unit circle is $\tau = \zeta, \tau = z$ and $\tau = z^{\frac{1}{3}}\omega^j$ for $j = 1, 2, 3$ and $\omega = e^{\frac{2\pi i}{3}}$ describes the 3-root of unity.

Setting $z_1 = z, z_2 = \zeta$ in equation (41), we can compute the Hilbert series.

$$\begin{aligned}H(R, z, \zeta) =& \mathrm{Res}(P, \tau = z) + \mathrm{Res}(P, \tau = \zeta) + \sum_{j=1}^{3} \mathrm{Res}(P, \tau = z^{\frac{1}{3}}\omega^j)\\ =& \frac{1 + z^3\zeta^3}{(1 - z\zeta^3)(1 - z^4)(1 - z^2\zeta^2)}\\ =& 1 + z\zeta^3 + z^2\zeta^2 + z^3\zeta^3 + z^4 + \cdots\end{aligned}$$

implying the fundamental invariants consist of the invariant 1 and three other: one that is of degree 1 in **a** and 3 in **b**, one of degree 2 both in **a** and **b**, one of degree 3 both in **a** and **b**, one of degree 4 in **a** and 0 in **b**. Also,

$$\begin{aligned}H(R, z, \zeta) =& \frac{1}{(1 - z\zeta^3)(1 - z^4)(1 - z^2\zeta^2)} + z^3\zeta^3\frac{1}{(1 - z\zeta^3)(1 - z^4)(1 - z^2\zeta^2)}\\ =& (1 + z\zeta^3 + z^4 + z^2\zeta^2 + \cdots) + z^3\zeta^3(1 + z\zeta^3 + z^4 + z^2\zeta^2 + \cdots)\end{aligned}$$

implying there are two secondary invariants: the invariant 1 and another of degree 3 in both **a** and **b** and three primary invariants, one of degree 1 in **a** and 3 in **b**, one of degree 4 in **a** and one of degree 2 in both **a** and **b**. In other words, $k = 3, s = 1$.

It remains to generate invariants of the desired degree. We can exploit the method of transvections to generate covariants since all covariants can be generated by the method of transvections. We then then transform these covariants into simultaneous invariants.

The form $\mathcal{F}$ itself is a covariant. By theorem 10), we can form an invariant of degree 1 in **a** and degree 2 in **b**:

$$f = a_0 b_1^3 - 3a_0 b_1^2 b_0 + 3a_0 b_1 b_0^2 - b_0^3. \tag{43}$$

Using transvections, i.e. formula (23), we can form the other covariants, and therefore invariants:

$$\begin{aligned}
f_2 = (\mathcal{F}, \mathcal{F})_2 =& (a_0 a_2 - a_1^2) x_1^2 + (a_3 a_0 - a_1 a_2) x_1 x_2 + (a_1 a_3 - a_2^2) x_2^2 \\
H =& (a_0 a_2 - a_1^2) b_1^2 - (a_3 a_0 - a_1 a_2) b_1 b_0 + (a_1 a_3 - a_2^2) b_0^2 \\
& \text{by theorem (10)} \\
D = -4(f_2, f_2)_2 =& a_3^2 a_0^2 - 6a_0 a_1 a_2 a_3 - 3a_1^2 a_2^2 + 4a_0 a_2^3 + 4a_1^3 a_3 \\
& \text{note that this is also the discriminant for the cubic form.} \\
2(f_2, \mathcal{F})_1 =& (a_0^2 a_3 - 3a_0 a_1 a_2 + 2a_1^3) x_1^3 + (3a_0 a_1 a_3 - 6a_0 a_2^2 + 3a_1^2 a_2) x_1^2 x_2 - \\
& (3a_0 a_2 a_3 - 6a_1^2 a_3 + 3a_1 a_2^2) x_1 x_2^2 - (a_0 a_3^2 - 3a_1 a_2 a_3 + 2a_2^3) x_2^3 \\
j =& (a_0^2 a_3 - 3a_0 a_1 a_2 + 2a_1^3) b_1^3 - (3a_0 a_1 a_3 - 6a_0 a_2^2 + 3a_1^2 a_2) b_1^2 b_0 \\
& - (3a_0 a_2 a_3 - 6a_1^2 a_3 + 3a_1 a_2^2) b_1 b_0^2 + (a_0 a_3^2 - 3a_1 a_2 a_3 + 2a_2^3) b_0^3
\end{aligned}$$

Hence, $f, D, H$ are our candidates for primary invariants and $j, 1$ our secondary invariant. However, the set of primary invariants have to be algebraically independent and the set of secondary invariants have to be linearly independent over the primary ones. We shall check the independence properties of $f, H, D, j$ using Groebner basis with the aid of *slack variables*.

Consider the set $\{f - \alpha_1, H - \alpha_2, D - \alpha_3, j - \alpha_4\}$. The Groebner basis for this set contains only one element that is entirely in terms of the $\alpha$'s. That is $\alpha_1^2 \alpha_3 - 4\alpha_2^3 - \alpha_4^2$. Setting $\alpha_1^2 \alpha_3 - 4\alpha_2^3 - \alpha_4^2 = 0$ gives the algebraic relationship between $f, H, D, j$, i.e. the syzygy $f^2 D - 4H^3 = j^2$. The $\alpha$'s is called the *slack variables*. This is an example of another useful application of Groebner basis [11]. This single syzygy gives the only relationship among $f, H, D, j$ and the expression of the syzygy suggests that $f, D, H$ are algebraically independent and $jand1$ are linearly independent over $f, D, H$.

Hence, $\{f, D, H\}$ is a working set of primary invariants while $j, 1$ are perfectly good choices as the secondary invariant. Then, every $P \in R$ can be written uniquely in terms for the Hironaka decomposition

$$P = P_0(f, H, D) + jP_1(f, H, D)$$

where $P_0, P_1$ are polynomials in their variables. We can also double check that the ring generated by $f, H, D, j$ in the form of this decomposition, call it $R'$, is the ring $R$, since $R' \subseteq R$ and they have the same Hilbert series, i.e. $\dim(R_{\mathbf{g},p}) = \dim(R'_{\mathbf{g},p})$ for all $\mathbf{g}, p$.

# 5 Connection with Normal Form Computation

We shall consider normal forms for bifurcation problems. Hence, we assume that a center manifold reduction has been employed and we can restrict our attention to dynamics on center manifolds. That is to say, the linearized operator should have eigenvalues with zero real parts. Hence, we consider only matrices whose eigenvalues are either zero or purely imaginary.

## 5.1 Zero Eigenvalues with Multiplicities

We consider matrices with zero eigenvalues of geometric multiplicity $k$ and algebraic multiplicities $n_1 + 1, n_2 + 1, \cdots, n_k + 1$. That is the matrix is

$$L_0 = \begin{pmatrix} \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & & 0 \end{pmatrix}_{(n_1+1)\times(n_1+1)} & & \\ & \ddots & \\ & & \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & & 0 \end{pmatrix}_{(n_k+1)\times(n_k+1)} \end{pmatrix}.$$

The normal form $F$ is characterized by the homological equation

$$H_{\mathbf{x}}F = (L_0^*\mathbf{x}) \cdot D_{\mathbf{x}}F = L_0^*F$$

where

$$\mathbf{x} = \left(x_1^{(1)}, x_2^{(1)}, \cdots, x_{n_1+1}^{(1)}, x_1^{(2)}, \cdots, x_{n_2+1}^{(2)}, \cdots, x_1^{(k)}, \cdots, x_{n_k+1}^{(k)}\right)$$

and

$$F = \left(F_0^{(1)}, F_1^{(1)}, \cdots, F_{n_1}^{(1)}, F_0^{(2)}, \cdots, F_{n_2}^{(2)}, \cdots, F_0^{(k)}, \cdots, F_{n_k}^{(k)}\right).$$

That is,

$$\left\{\left(x_1^{(1)}\frac{\partial}{\partial x_2^{(1)}} + x_2^{(1)}\frac{\partial}{\partial x_3^{(1)}} + \cdots + x_{n_1}^{(1)}\frac{\partial}{\partial x_{n_1+1}^{(1)}}\right) + \cdots + \left(x_1^{(k)}\frac{\partial}{\partial x_2^{(k)}} + x_2^{(k)}\frac{\partial}{\partial x_3^{(k)}} + \cdots + x_{n_k}^{(k)}\frac{\partial}{\partial x_{n_k+1}^{(k)}}\right)\right\} \begin{pmatrix} F_0^{(1)} \\ F_1^{(1)} \\ \vdots \\ F_{n_1}^{(1)} \\ \vdots \\ F_0^{(k)} \\ F_1^{(k)} \\ \vdots \\ F_{n_k}^{(k)} \end{pmatrix} = \begin{pmatrix} 0 \\ F_0^{(1)} \\ \vdots \\ F_{n-1}^{(1)} \\ \vdots \\ 0 \\ F_0^{(k)} \\ \vdots \\ F_{n_k}^{(k)} \end{pmatrix} \tag{44}$$

Suppose we make a change of variables

$$x_1^{(1)} = a_0, x_2^{(1)} = \frac{a_1}{1!}, x_3^{(1)} = \frac{a_2}{2!}, \cdots, x_{n_1+1}^{(1)} = \frac{a_{n_1}}{(n_1)!};$$

$$x_1^{(2)} = b_0, x_2^{(2)} = \frac{b_1}{1!}, x_3^{(2)} = \frac{b_2}{2!}, \cdots, x_{n_2+1}^{(2)} = \frac{b_{n_2}}{(n_2)!};$$

$$\vdots$$

$$x_1^{(k)} = w_0, x_2^{(k)} = \frac{w_1}{1!}, x_3^{(k)} = \frac{w_2}{2!}, \cdots, x_{n_k+1}^{(k)} = \frac{w_{n_k}}{(n_k)!}.$$

Then,

$$\begin{aligned}
H_{\mathbf{x}} =& \left( x_1^{(1)} \frac{\partial}{\partial x_2^{(1)}} + x_2^{(1)} \frac{\partial}{\partial x_3^{(1)}} + \cdots + x_{n_1}^{(1)} \frac{\partial}{\partial x_{n_1+1}^{(1)}} \right) + \cdots + \\
& \left( x_1^{(k)} \frac{\partial}{\partial x_2^{(k)}} + x_2^{(k)} \frac{\partial}{\partial x_3^{(k)}} + \cdots + x_{n_k}^{(k)} \frac{\partial}{\partial x_{n_k+1}^{(k)}} \right) \\
=& \left( a_0 \frac{\partial}{\partial a_1} + 2a_1 \frac{\partial}{\partial a_2} + \cdots + n_1 a_{n_1-1} \frac{\partial}{\partial a_{n_1}} \right) + \cdots + \\
& \left( w_0 \frac{\partial}{\partial w_1} + 2w_1 \frac{\partial}{\partial w_2} + \cdots + n_k w_{n_k-1} \frac{\partial}{\partial w_{n_k}} \right) \\
=& \mathbf{D_a} + \mathbf{D_b} + \cdots + \mathbf{D_w} \\
=& \mathbf{D}
\end{aligned}$$

corresponds to a system of $k$ binary forms of order $n_1, n_2, \cdots, n_k$ respectively, i.e.

$$\begin{aligned}
\mathcal{F}_1 =& a_0 y_1^{n_1} + \binom{n_1}{1} a_1 y_1^{n_1-1} y_2 + \cdots + a_{n_1} y_2^{n_1} \\
\mathcal{F}_2 =& b_0 y_1^{n_2} + \binom{n_2}{1} b_1 y_1^{n_2-1} y_2 + \cdots + b_{n_2} y_2^{n_2} \\
& \vdots \\
\mathcal{F}_k =& w_0 y_1^{n_k} + \binom{n_k}{1} w_1 y_1^{n_k-1} y_2 + \cdots + w_{n_k} y_2^{n_k}
\end{aligned}$$

In our previous method of computing normal form in chapter **??**, the fundamental task was to find a solution $q$ to the scalar differential equation $H_{\mathbf{x}} q = 0$ where $q$ is polynomial in $\mathbf{x}$. Now, we see that the problem of finding such a $q$ is equivalent to finding a simultaneous covariant $\mathcal{C}$ to the above system of forms, such that the source $C_0$ satisfies $\mathbf{D}C_0 = 0$.

Let $R$ be the graded ring that consists of all polynomials in $\mathbf{a}, \mathbf{b}, \cdots, \mathbf{w}$ that satisfy the differential equation $\mathbf{D}f = 0$ for $f \in R$. Note that $R$ contains all sources of covariants in $\mathbf{a}, \mathbf{b}, \cdots, \mathbf{w}$ since if $C_0$ is the source of a covariant in $\mathbf{a}, \mathbf{b}, \cdots, \mathbf{w}$, then $C_0$ satisfies $\mathbf{D}C_0 = 0$.

We wish to find a unique representation for $R$. To do this, we need to be able to use the notions of invariants and covariants interchangably. This can be done since covariants can be thought of as simultaneous invariants if one is willing to include an extra linear form into the system of forms. We shall first address these general basic issues.

Let $R_{\mathbf{g},p}$ be the graded subring consists of homogeneous and isobaric polynomials of degree $\mathbf{g}$ and weight $p$. Note that $R = \bigoplus_{\mathbf{g},p} R_{\mathbf{g},p}$. It is enough to consider $R_{\mathbf{g},p}$ since any $f \in R$ can be written as a linear combination of homogenous and isobaric functions, i.e. $f = \sum_{\mathbf{g},p} f_{\mathbf{g},p}$ where $f_{\mathbf{g},p} \in R_{\mathbf{g},p}$. Then, $\mathbf{D}f = 0$ implies $\mathbf{D}f_{\mathbf{g},p} = 0$.

By theorem (9), if $C_0 \in R_{\mathbf{g},p}$ satisfying $\mathbf{D}C_0 = 0$ and $\mathbf{n}\cdot\mathbf{g} - 2p = m$, then there is a unique covariant $\mathcal{C}$ with source $C_0$ i.e.

$$\mathcal{C} = C_0 y_1^m + \frac{1}{1!}\Delta C_0 y_1^{m-1} y_2 + \frac{1}{2!}\Delta^2 C_0 y_1^{m-2} y_2^2 + \cdots + \frac{1}{m!}\Delta^m C_0 y_2^m.$$

Also, by theorem (10), this covariant can be made into a simultaneous invariant by adding a linear form $vy_1 - uy_2$ to the system of forms and then replacing $y_1$ by $u$ and $y_2$ by $v$. We summarize this as a proposition:

**Proposition 5.** *If $C_0 \in R_{\mathbf{g},p}$, $C_0 \neq 0$ satisfying $\mathbf{D}C_0 = 0$ and $\mathbf{n}\cdot\mathbf{g} - 2p = m \geq 0$, then there is an invariant*

$$\mathcal{I} = C_0 u^m + \Delta C_0 u^{m-1} v + \frac{1}{2!}\Delta^2 C_0 u^{m-2} v^2 + \cdots + \frac{1}{m!}\Delta^m C_0 v^m, \qquad (45)$$

*that satisfies*

$$\mathbf{D}_I \mathcal{I} = \left(\mathbf{D} - v\frac{\partial}{\partial u}\right)\mathcal{I} = 0$$

*and $\mathbf{n}'\cdot\mathbf{g}' - 2p' = 0$ where $n' = (n, 1)$, $g' = (\mathbf{g}, \deg$ in $(u, v))$ and $p' = p + \deg(u)$ if we assign weight 0 to $v$ and weight 1 to $u$.*

**Remark 2.** *We can recover $C_0$ from $\mathcal{I}$ by setting $u = 1$ and $v = 0$ in $\mathcal{I}$.*

Let $R_I$ be the ring of invariants with $\mathbf{D}_I\mathcal{I} = \left(\mathbf{D} - v\frac{\partial}{\partial u}\right)\mathcal{I} = 0$ for $\mathcal{I} \in R_I$. Then there is an isomorphism

$$R \underset{T_b}{\overset{T_f}{\rightleftarrows}} R_I$$

such that

$$\begin{aligned} T_f(C_0) =& C_0 u^m + \Delta C_0 u^{m-1} v + \frac{1}{2!}\Delta^2 C_0 u^{m-2} v^2 + \cdots + \frac{1}{m!}\Delta^m C_0 v^m \\ & \text{with } m = \mathbf{n}\cdot\mathbf{g} - 2p; \\ T_b(\mathcal{I}) =& T_b(\mathcal{I}(\mathbf{a}, \mathbf{b}, \cdots, \mathbf{w}, u, v)) = \mathcal{I}(\mathbf{a}, \mathbf{b}, \cdots, \mathbf{w}, 1, 0). \end{aligned}$$

By theorem 18, $R_I$ is Cohen-Macaulay and has a Hironaka decomposition. This means, there exist algebraically independent primary invariants

$\theta_1, \theta_2, \cdots, \theta_r$ and secondary invariants $\eta_1, \eta_2, \cdots, \eta_s$ that are linearly independent over the primary invariants, such that every $f \in R_I$ is uniquely represented by

$$f = \eta_1 P_1(\theta_1, \cdots, \theta_r) + \eta_2 P_2(\theta_1, \cdots, \theta_r) + \cdots \eta_s P_s(\theta_1, \cdots, \theta_r).$$

The existence of such a finite set of primary and secondary invariants implies $R$ has a finite basis.

Since $R_I$ is Cohen-Macaulay, the Hilbert series takes the form, as in 37

$$H(R, \mathbf{z}) = \sum_{\mathbf{g}} \dim(R_{\mathbf{g}}) \mathbf{z}^{\mathbf{g}} = \frac{\mathbf{z}^{\mathbf{g}_1''} + \mathbf{z}^{\mathbf{g}_2''} + \cdots + \mathbf{z}^{\mathbf{g}_s''}}{(1 - \mathbf{z}^{\hat{\mathbf{g}}_1})(1 - \mathbf{z}^{\hat{\mathbf{g}}_2}) \cdots (1 - \mathbf{z}^{\hat{\mathbf{g}}_r})}$$

The Hilbert series suggests that the $r$ primary invariants are homogeneous in degree $\hat{\mathbf{g}}_1, \hat{\mathbf{g}}_2, \cdots, \hat{\mathbf{g}}_r$ respectively; and the $s$ secondary invariants are of degree $\mathbf{g}_1'', \mathbf{g}_2'', \cdots, \mathbf{g}_s''$.

**Remark 3.** *The Hilbert series for the system of forms $\mathcal{F}_1, \mathcal{F}_2, \cdots, \mathcal{F}_k, l$ can be calculated using equation 41.*

Hence, it suffices to find $r$ algebraically independent invariants of degrees $\hat{\mathbf{g}}_1, \cdots, \hat{\mathbf{g}}_r$. These will be our primary invariants. Then, we need to find $s$ invariants of degrees $\mathbf{g}_1'', \cdots, \mathbf{g}_s''$ that are linearly independent of our set of primary invariants. These will be the secondary invariants. We will then obtain the desired decomposition.

We generate invariants from covariants that are in turn generated by taking transvections. We start with the forms $\mathcal{F}_1, \cdots, \mathcal{F}_k$ that are themselves covariants. Using the appropriate $p$-transvections, we can generate all other relevent covariants. We then apply $T_f$ to all these covariants to obtain the corresponding invariants of desired degrees $\hat{\mathbf{g}}_1, \cdots, \hat{\mathbf{g}}_r, \mathbf{g}_1'', \cdots, \mathbf{g}_s''$, i.e. $\theta_1, \theta_2, \cdots, \theta_r, \eta_1, \cdots, \eta_s$.

$\theta_1, \cdots, \theta_r$ are candidates for primary invariants. For these $\theta_i$ to be primary invariants, they need to be an algebraically independent set. Similarly, $\eta_1, \cdots, \eta_s$ are potential secondary invariants. For them to be secondary invariants, they have to be linearly independent over the primary invariants. To verify the independence property of our candidates, we use Groebner basis with the aid of slack variables as in example 4.8 to identify all possible relations among the $\theta_i$ and $\eta_j$ for all $i = 1, \cdots, r$, $j = 1, \cdots, s$.

Once we obtain a set of $r$ algebraically independent invariants $\theta_1, \cdots, \theta_r$ and a set of $s$ invariants $\eta_1, \cdots, \eta_s$ that are linearly independent over the $\theta$'s, then $R_I$ is representable as

$$f = \eta_1 P_1(\theta_1, \cdots, \theta_r) + \eta_2 P_2(\theta_1, \cdots, \theta_r) + \cdots \eta_s P_s(\theta_1, \cdots, \theta_r),$$

for all $f \in R_I$.

If we now make the substitution $u = 1, v = 0$, $a_0 = x_1^{(1)}, a_1 = x_2^{(1)}, a_2 = 2!x_3^{(1)}, \cdots, a_i = i!x_{i+1}^{(1)}, \cdots, a_{n_1} = (n_1)!x_{n_1+1}^{(1)}, b_0 = x_1^{(2)}, \cdots, b_{n_2} = (n_2)!x_{n_2+1}^{(2)}, \cdots w_{n_k} = (n_k)!x_{n_k+1}^{(k)}$, then any $f$ satisfying $H_{\mathbf{x}} f = 0$ can be represented uniquely by

$$\begin{aligned} f(\mathbf{x}) =& \eta_1(\mathbf{a}(\mathbf{x}), \mathbf{b}(\mathbf{x}), \cdots, \mathbf{w}(\mathbf{x})) P_1(\theta_1(\mathbf{a}(\mathbf{x}), \cdots, \mathbf{w}(\mathbf{x})), \cdots, \theta_r(\mathbf{a}(\mathbf{x}), \cdots, \mathbf{w}(\mathbf{x}))) \\ &+ \eta_2(\mathbf{a}(\mathbf{x}), \cdots, \mathbf{w}(\mathbf{x})) P_2(\theta_1(\mathbf{a}(\mathbf{x}), \cdots, \mathbf{w}(\mathbf{x})), \cdots, \theta_r(\mathbf{a}(\mathbf{x}), \cdots, \mathbf{w}(\mathbf{x}))) \\ &+ \cdots \eta_s(\mathbf{a}(\mathbf{x}), \cdots, \mathbf{w}(\mathbf{x})) P_s(\theta_1(\mathbf{a}(\mathbf{x}), \cdots, \mathbf{w}(\mathbf{x})), \cdots, \theta_r(\mathbf{a}(\mathbf{x}), \cdots, \mathbf{w}(\mathbf{x}))). \end{aligned}$$

**Example 11.** *Consider the case of 4 zero eigenvalues, i.e.*

$$L_0 = \begin{pmatrix} 0 & 1 & & \\ & 0 & 1 & \\ & & \ddots & \ddots \\ & & & 0 \end{pmatrix}.$$

*The homological operator is*

$$H_x = x_1 \frac{\partial}{\partial x_2} + x_2 \frac{\partial}{\partial x_3} + x_3 \frac{\partial}{\partial x_4}.$$

*This corresponds to the operator* $\mathbf{D}$ *for the binary form*

$$\mathcal{F} = a_0 y_1^3 + a_1 y_1^2 y_2 + a_2 y_1 y_2^2 + a_3 y_2^2.$$

*We shall introduce the linear binary form*

$$l = b_0 x_1 + b_1 x_2$$

*so that we can consider covariants in terms of simultaneous invariants. Note that this is the exact same system of forms we considered in detail in section 4.8. Hence, we know that every invariant can be written uniquely as*

$$\mathcal{I} = P_0(t, H, D) + j P_1(t, H, D)$$

*where*

$$\begin{aligned} t =& a_0 b_1^3 - 3a_0 b_1^2 b_0 + 3a_0 b_1 b_0^2 - b_0^3 \\ H =& (a_0 a_2 - a_1^2) b_1^2 - (a_3 a_0 - a_1 a_2) b_1 b_0 + (a_1 a_3 - a_2^2) b_0^2 \\ D =& a_3^2 a_0^2 - 6a_0 a_1 a_2 a_3 - 3a_1^2 a_2^2 + 4a_0 a_2^3 + 4a_1^3 a_3 \\ j =& (a_0^2 a_3 - 3a_0 a_1 a_2 + 2a_1^3) b_1^3 - (3a_0 a_1 a_3 - 6a_0 a_2^2 + 3a_1^2 a_2) b_1^2 b_0 \\ &- (3a_0 a_2 a_3 - 6a_1^2 a_3 + 3a_1 a_2^2) b_1 b_0^2 + (a_0 a_3^2 - 3a_1 a_2 a_3 + 2a_2^3) b_0^3 \end{aligned}$$

*Substituting* $b_1 = 1, b_0 = 0, a_0 = x_1, a_1 = x_2, a_2 = 2x_3, a_3 = 6x_4$, *we have*

$$\begin{aligned} t &= x_1 \\ H &= 2x_1x_3 - x_2^2 \\ D &= 36x_4^2x_1^2 - 72x_1x_2x_3x_4 - 12x_2^2x_3^2 + 32x_1x_3^3 + 24x_2^3x_4 \\ &= 4(9x_1^2x_4^2 - 18x_1x_2x_3x_4 - 3x_2^2x_3^2 + 8x_1x_3^3 + 6x_2^3x_4) \\ j &= 6x_1^2x_4 - 6x_1x_2x_3 + 2x_2^3 \\ &= 2(x_2^3 + 3x_1^2x_4 - 3x_1x_2x_3) \end{aligned}$$

*In the notation of the old technique,* $t = u_1, H = -u_3, D = 4u_6, j = 2u_4$. *This confirms the calculation that* $F_0 = \phi_0(u_1, u_3, u_6) + u_4\phi_1(u_1, u_3, u_6)$ *where* $\phi_0, \phi_1$ *are polynomials in their variables.*

This is not the whole story. In this section, we will attempt to address the vector differential equation, i.e. the homological equation:

$$H_{\mathbf{x}}F = L_0^*F.$$

First, note that each block $F_0^{(i)}, F_1^{(i)}, \cdots, F_{n_i}^{(i)}$ satisfies similar homological equation, i.e.

$$H_{\mathbf{x}} \begin{pmatrix} F_0^{(i)} \\ F_2^{(i)} \\ \vdots \\ F_{n_i}^{(i)} \end{pmatrix} = \begin{pmatrix} 0 \\ F_0^{(i)} \\ \vdots \\ F_{n_i-1}^{(i)} \end{pmatrix}$$

Hence, we shall work with one such block and drops the $i$ dependence. Let

$$G_j = G_j(\mathbf{a}, \mathbf{b}, \cdots, \mathbf{w}) = F_j\left(x_1^{(1)}(a_0), \cdots, x_{n_1+1}^{(1)}(a_{n_1}), \cdots, x_{n_k+1}^{(k)}(w_{n_k})\right).$$

Then,

$$H_{\mathbf{x}}F = L_0^*F \Rightarrow \mathbf{D}G = L_0^*G.$$

Consider

$$\mathbf{D}\begin{pmatrix} G_0 \\ G_1 \\ \vdots \\ G_n \end{pmatrix} = L_0^*\begin{pmatrix} G_0 \\ G_1 \\ \vdots \\ G_n \end{pmatrix} = \begin{pmatrix} 0 \\ G_0 \\ \vdots \\ G_{n-1} \end{pmatrix}$$

This means

$$\begin{aligned}\mathbf{D}G_0 =& 0\\ \mathbf{D}G_1 =& G_0\\ \mathbf{D}^2G_2 =& G_0\\ &\vdots\\ \mathbf{D}^nG_n =& G_0\end{aligned}$$

Hence, to characterize $G_0$, we not only need $G_0 \in \ker(\mathbf{D})$, we need

$$G_0 \in \ker(\mathbf{D}) \cap \text{Image}(\mathbf{D}) \cap \text{Image}(\mathbf{D}^2) \cap \cdots \cap \text{Image}(\mathbf{D}^n).$$

However, $\text{Image}(\mathbf{D}^n) \subset \text{Image}(\mathbf{D}^{n-1}) \subset \cdots \subset \text{Image}(\mathbf{D})$. Hence, it's enough to seek $G_0 \in \ker(\mathbf{D}) \cap \text{Image}(\mathbf{D}^n)$.

Conversely, if $\phi \in \ker(\mathbf{D}) \cap \text{Image}(\mathbf{D}^n)$, then

$$\mathbf{D}\phi = 0 \text{ and } \exists\, \psi \text{ such that } \mathbf{D}^n\psi = \phi.$$

Now, define

$$\begin{pmatrix} G_0\\ G_1\\ G_2\\ \vdots\\ G_n \end{pmatrix} = \begin{pmatrix} \phi\\ \mathbf{D}^{n-1}\psi\\ \mathbf{D}^{n-2}\psi\\ \vdots\\ \psi \end{pmatrix}.$$

Then,

$$\begin{aligned}\mathbf{D}G_0 =& \mathbf{D}\psi = 0\\ \mathbf{D}G_1 =& \mathbf{D}\left(\mathbf{D}^{n-1}\psi\right) = \mathbf{D}^n\psi = \phi = G_0\\ \mathbf{D}^2G_2 =& \mathbf{D}\left(\mathbf{D}^{n-2}\psi\right) = \mathbf{D}^n\psi = G_0\\ &\vdots\\ \mathbf{D}^nG_n =& \mathbf{D}^n\psi = G_0\end{aligned}$$

hence solving the equation

$$\mathbf{D}G = L_0^*G.$$

**Proposition 6.** *If $C_0 \in R_{\mathbf{g},p}$ where $R_{\mathbf{g},p}$ is the multi-graded subring of homogeneous polynomial of degree $\mathbf{g}$ and weight $p$, $C_0 \neq 0$ and $\mathbf{n}\cdot\mathbf{g} - 2p = m$, then*

$$m \geq 0,\ C_0 \in \text{Image}(\mathbf{D}^m) \quad \textit{and} \quad C_0 \notin \text{Image}(\mathbf{D}^{m+1}).$$

*Proof.* First, note that for a homogeneous function $\mathcal{A}$, of degree $\mathbf{g}$ and weight $p$, the operators $\mathbf{D}$ and $\Delta$ have another commutator, similar to but different from that in equation (33):

$$(\mathbf{D}\Delta^k - \Delta^k\mathbf{D})\mathcal{A} = k(\mathbf{n}\cdot\mathbf{g} - 2p - k + 1)\Delta^{k-1}\mathcal{A} \tag{46}$$

If $\mathbf{D}\mathcal{A} = 0$, we have

$$\mathbf{D}(\Delta^k\mathcal{A}) = k(\mathbf{n}\cdot\mathbf{g} - 2p - k + 1)\Delta^{k-1}\mathcal{A}.$$

Applying the operator $\mathbf{D}$ inductively to both sides of the equation $q$ times yields

$$\begin{aligned}\mathbf{D}^q(\Delta^k\mathcal{A}) =& k(k-1)(k-2)\cdots(k-q+1)(\mathbf{n}\cdot\mathbf{g} - 2p - k + 1)(\mathbf{n}\cdot\mathbf{g} - 2p - k + 2)\cdots \\ & (\mathbf{n}\cdot\mathbf{g} - 2p - k + q)\Delta^{k-q}\mathcal{A}\end{aligned} \tag{47}$$

for $1 \le q \le k$.

Note that similar calculation using equation (33) yields a similar identity

$$\begin{aligned}\Delta^q(\mathbf{D}^k\mathcal{A}) =& k(k-1)(k-2)\cdots(k-q+1)(\mathbf{n}\cdot\mathbf{g} - 2p + k - 1)(\mathbf{n}\cdot\mathbf{g} - 2p + k - 2)\cdots \\ & (\mathbf{n}\cdot\mathbf{g} - 2p + k - q)\mathbf{D}^{k-q}\mathcal{A}\end{aligned} \tag{48}$$

for $1 \le q \le k$.

To show $m \ge 0$, consider the sequence

$$C_0, \Delta C_0, \Delta^2 C_0, \cdots, \Delta^{k-1}C_0, \Delta^k C_0$$

such that $\Delta^{k-1}C_0 \neq 0$ but $\Delta^k C_0 = 0$. Such a $k$ exists because the operator $\Delta$ increases the weight by 1 (but preserves degree) in each application. For a polynomial of fixed degree with a fixed number of variables, there is a finite maximum for the weight. Hence, the weight has to saturate after sufficient applications of $\Delta$. From previous paragaraph

$$\begin{aligned}\left(\mathbf{D}\Delta^k - \Delta^k\mathbf{D}\right)C_0 =& k(\mathbf{n}\cdot\mathbf{g} - 2p - k + 1)\Delta^{k-1}C_0 \\ 0 =& k(m + 1 - k)\Delta^{k-1}C_0.\end{aligned}$$

Since $C_0 \neq 0$, $k \neq 0$. Also, $\Delta^{k-1}C_0 \neq 0$. Hence, we must have $m - k + 1 = 0$. However, $m \ge 0$ since $k \ge 1$ (because otherwise $C_0 = 0$).

Next, we will show that $C_0 \in \text{Image}(\mathbf{D}^m)$. From equation (47), we have

$$\mathbf{D}^m(\Delta^m C_0) = (m!)^2 C_0.$$

Since $(m!)^2 \neq 0$, we necessarily have $C_0 \in \text{Image}(\mathbf{D}^m)$. Note that $C_0 \in \text{Image}(\mathbf{D}^k)$ for all $k \leq m$ by the same argument.

Finally, we shall show that $C_0 \notin \text{Image}(\mathbf{D}^{m+1})$ by contradiction. Assume there is an $A$ such that $C_0 = \mathbf{D}^{m+1}A$. $A$ has degree $\mathbf{g}$ and weight $p' = p - m - 1$. Hence, $\mathbf{n} \cdot \mathbf{g} - 2p' = \mathbf{n} \cdot \mathbf{g} - 2p - 2m - 2 = m - 2m - 2 = -m - 2$.

Let $k \geq 0$ be such that $B = \Delta^k A \neq 0$ but $\Delta B = 0$. Then, $B$ has degree $\mathbf{g}$ since the operators $\mathbf{D}$ and $\Delta$ both preserve degree. Also, $B$ has weight $p'' = p + (m+1) + k$. Hence,

$$\mathbf{n} \cdot \mathbf{g} - 2p' = \mathbf{n} \cdot \mathbf{g} - 2p - 2(k + 1 + m) = -m - 2k - 2.$$

Now, by equation (48),

$$\begin{aligned}
\Delta^{m+k+2}(\mathbf{D}^{m+k+2}B) =& (m+k+2)! \cdot (\mathbf{n} \cdot \mathbf{g} - 2p'' + m + 2 + k - 1) \\
& (\mathbf{n} \cdot \mathbf{g} - 2p'' + m + 2 + k - 2) \cdots (\mathbf{n} \cdot \mathbf{g} - 2p'')B \\
=& (m+k+2)!(-k-1)(-k-2)\cdots(-m-2k-2)B \\
=& (m+k+2)!(-1)^{m+k+2}\frac{(m+k+2)!}{k!}B \neq 0, \text{ since } B \neq 0
\end{aligned}$$

This implies $\mathbf{D}^{m+k+2}B \neq 0$. However, this cannot be true because

$$\begin{aligned}
\mathbf{D}^{m+k+2}B =& \mathbf{D}\left(\mathbf{D}^{m+1}(\mathbf{D}^k B)\right) \\
=& \mathbf{D}\left(\mathbf{D}^{m+1}(\mathbf{D}^k(\Delta^k A))\right) \\
=& \mathbf{D}\left(\mathbf{D}^{m+1}\left(k!(\mathbf{n} \cdot \mathbf{g} - 2p' - k + 1)(\mathbf{n} \cdot \mathbf{g} - 2p' - k + 2)\cdots(\mathbf{n} \cdot \mathbf{g} - 2p')A\right)\right) \\
=& \mathbf{D}\left(\mathbf{D}^{m+1}\left(k!(-m-2-k+1)(-m-2-k+2)\cdots(-m-2)A\right)\right) \\
=& (-1)^k \frac{k!(m+k+1)!}{(m+1)!}\mathbf{D}\left(\mathbf{D}^{m+1}A\right) \\
=& (-1)^k \frac{k!(m+k+1)!}{(m+1)!}\mathbf{D}C_0 = 0
\end{aligned}$$

Hence, $C_0 \notin \text{Image}(\mathbf{D}^{m+1})$. In fact, similar argument can be used to show that $C_0 \notin \text{Image}(\mathbf{D}^k)$ for all $k \geq m+1$. □

Note that

$$\begin{aligned}\ker(\mathbf{D}) \cap \text{Image}(\mathbf{D}^k) =& R \cap \text{Image}(\mathbf{D}^k) \\ =& \bigoplus_{\mathbf{g},p} R_{\mathbf{g},p} \cap \text{Image}(\mathbf{D}^k) \\ =& \begin{cases} R_{\mathbf{g},p} & \text{if } k \le \mathbf{n}\cdot\mathbf{g} - 2p \\ \{0\} & \text{if } k > \mathbf{n}\cdot\mathbf{g} - 2p. \end{cases} \\ =& \bigoplus_{\mathbf{g},p\,|\mathbf{n}\cdot\mathbf{g}-2p\ge k} R_{\mathbf{g},p}\end{aligned}$$

The isomorphisms $T_f$ and $T_b$ gives a one-to-one correspondence between elements of $\ker(\mathbf{D}) \cap \text{Image}(\mathbf{D}^k)$ and elements of $R_I$ with $m \ge k$ where $m = \mathbf{n}\cdot\mathbf{g} - 2p$ is the degree of $(u, v)$ in $\mathcal{I} \in R_I$, (45).

## 5.2 Purely Imaginary Eigenvalues with Multiplicities

For matrices with purely imaginary eigenvalues $\pm i\omega$ with algebraic multiplicity $n$, the $2n \times 2n$ matrix can be written as a sum of its semisimple and nilpotent parts:

$$L = \begin{pmatrix} +i\omega & 1 & & & & & & & & \\ & +i\omega & 1 & & & & & & & \\ & & \ddots & \ddots & & & & & & \\ & & & & +i\omega & & & & & \\ & & & & & -i\omega & 1 & & & \\ & & & & & & -i\omega & 1 & & \\ & & & & & & & \ddots & \ddots & \\ & & & & & & & & & -i\omega \end{pmatrix} = L_\omega + L_0$$

where

$$L_\omega = \begin{pmatrix} +i\omega & & & & & & & & \\ & \ddots & \ddots & & & & & & \\ & & & +i\omega & & & & & \\ & & & & -i\omega & & & & \\ & & & & & \ddots & \ddots & & \\ & & & & & & & & -i\omega \end{pmatrix}$$

and

$$L_0 = \begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & \ddots & \ddots & \\ & & & & 0 \end{pmatrix}.$$

# 6 An Alternate Derivation for Normal Forms

# References


[1] B. Buchberger. *An algorithm for finding a basis for the residue class ring of a zero-dimensional polynomial ideal*. PhD thesis, Institute for Mathematics, University of Innsbruck, 1965. German.

[2] D. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1997. An introduction to computational algebraic geometry and commutative algebra.

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

[4] C. Elphick, E. Tirapegui, M. E. Brachet, P. Coullet, and G. Iooss. A simple global characterization for normal forms of singular vector fields. *Phys. D*, 29(1-2):95–127, 1987.

[5] P. Gordan. Beweis, dass jede Covariante und Invariante einer binären Form eine ganze Funktion mit numerischen Coefficienten einer endlichen Anzahl solcher Formen ist. *J. Reine. Agnew. Math.*, 69:323–354, 1868.

[6] D. Hilbert. *Theory of algebraic invariants*. Cambridge University Press, Cambridge, 1993. Translated from the German and with a preface by Reinhard C. Laubenbacher, Edited and with an introduction by Bernd Sturmfels.

[7] M. Hochster and J. L. Roberts. Rings of invariants of reductive groups acting on regular rings are Cohen-Macaulay. *Advances in Math.*, 13:115–175, 1974.

[8] T. W. Hungerford. *Algebra*, volume 73 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1980. Reprint of the 1974 original.

[9] M. Reid. *Undergraduate commutative algebra*, volume 29 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1995.

[10] T. A. Springer. *Invariant theory*. Springer-Verlag, Berlin, 1977. Lecture Notes in Mathematics, Vol. 585.

[11] B. Sturmfels. *Algorithms in invariant theory*. Texts and Monographs in Symbolic Computation. Springer-Verlag, Vienna, 1993.