Theory of Algebraic Invariants

Lectures by

Prof. Hilbert

prepared by

Sophus Marxsen
cand. math.

Göttingen
Summer Semester 1897

I

The elements of invariant theory

Lecture I (April 27, 1897)

The theory of algebraic invariants, with which we want to concern ourselves here, is a modern discipline. Its origins can be traced back to Cayley (1845), who used the term "hyperdeterminants" for functions possessing the invariant property. At present, we only mention as references the four main text books which all differ from each other and treat the subject from different perspectives. These are the following:

Clebsch. *Theorie der binären algebraischen Formen.* Leibzig 1872.

Salmon. *Modern Higher Algebra.* Dublin 1885. German trans. by Friedler. Leibzig 1885.

Faà di Bruno. *Théorie des formes binaires.* Turin 1876. German trans. by Walter. Leibzig 1881.

Gordan. *Vorlesungen über Invariantentheorie.* Leibzig 1885 (in particular vol. II).

One should add to these: **Franz Meyer**, *Bericht über den gegenwärtigen Stand der Invariantentheorie*, 1892. (In the "Berichte der deutschen Mathematiker Vereinigung.")

The necessary prerequisite for an understanding of the following is a knowledge of differentiation and of the basic theorems from the theory of determinants. The latter can be found in, for example, **Bältzer**, *Determinantentheorie*; **Hasse**, *Raumgeometrie*, Lecture 7; **Salmon**, *Modern Higher Algebra*, Lecture 1; **Serret**, *Algèbre Supérieure*, Tome II, Ch. IV (of course also in the German translations); **H. Weber**, *Algebra*, vol. I, Sect. II.

The books by Salmon and Faà di Bruno are the best introduction to invariant theory.

I.1 The forms

A sum of products of constants and variables will be called a *polynomial.* Thus, if c_{ikl} are constants, and x, y, z are variables, then

$$\mathcal{F}(x,y,z) = \sum_{i,k,l} c_{ikl} x^i y^k z^l, \qquad i,k,l = 0,1,2,3,4,5,$$

is a polynomial in three variables. The general form of a polynomial is

$$\mathcal{F}(x,y,z,\ldots) = \sum_{i,k,l,\ldots} c_{ikl\ldots} x^i y^k z^l \cdots, \qquad i,k,l,\ldots = 0,1\ldots,n.$$

Each of the products, that is, each expression $c_{ikl\ldots}x^i y^k z^l \cdots$, is called a *term* of the polynomial. Its characteristic number $n = i + k + l + \cdots$, that is, the sum of the exponents of the variables, is called the *order of the term.* The order of the term with the highest order is called the *order of the polynomial.*

We always want to think of a polynomial as ordered, by taking first the term of order zero—the constant—then the terms of order one, then those of order two, etc; we want to indicate this by using the notation:

$$\mathcal{F}(x,y,z,\ldots) = [0] + [1] + [2] + \cdots + [n],$$

where n is the order of the polynomial.

The last term $[n]$ can not be identically zero, because otherwise the order would be smaller than n. On the other hand it is possible that all terms other than $[n]$ vanish, in which case the function is called a *homogeneous function* or a *form.* In this case, therefore, all terms have the same order.

In the following we will only consider forms. We want to introduce fixed notation for them, which we shall use throughout. The order of a form is always n (respectively, $\nu, N, \ldots$); the number of variables in general discussions will be m, so the variables will always be denoted $x_1, x_2, \ldots, x_m$.

It is no restriction to consider only forms, since we can always obtain a form from a polynomial and vice versa. Indeed, if we add a variable x_m to

$$\mathcal{F}(x_1, x_2, \ldots, x_{m-1}) = [0] + [1] + [2] + \cdots + [n],$$

then

$$\Phi(x_1, x_2, \ldots, x_m) = [0]x_m^n + [1]x_m^{n-1} + [2]x_m^{n-2} + \cdots + [n]$$

is a homogeneous function, from which we can easily reconstruct the original function by setting $x_m = 1$:

$$\Phi(x_1, x_2, \ldots, x_{m-1}, 1) = \mathcal{F}(x_1, x_2, \ldots, x_{m-1}).$$

Moreover, we have

$$x_m^n \mathcal{F}\left(\frac{x_1}{x_m}, \frac{x_2}{x_m}, \frac{x_3}{x_m}, \ldots, \frac{x_{m-1}}{x_m}\right) = \Phi(x_1, x_2, \ldots, x_m).$$

Hence, the theory of forms in m variables is essentially identical to the theory of general polynomials in $m-1$ variables. We will now derive two theorems which we will use frequently. Let

$$\Phi(x_1, x_2, \ldots, x_m) = \sum_{i,\ldots,s} c_{ik\ldots s} x_1^i x_2^k \cdots x_m^s, \qquad i + k + \cdots + s = n.$$

If we replace x_i by ux_i, where u is arbitrary, for example, a variable, then we obtain

$$\begin{aligned}\Phi(ux_1, \ldots, ux_m) &= \sum_{i,\ldots,s} c_{ik\ldots s} u^i x_1^i u^k x_2^k \cdots u^s x_m^s \\ &= \sum_{i,\ldots,s} c_{ik\ldots s} x_1^i x_2^k \cdots x_m^s u^{i+k+\cdots+s}.\end{aligned}$$

Therefore,

$$\Phi(ux_1, \ldots, ux_m) = u^n \sum_{i,\ldots,s} c_{ik\ldots s} x_1^i x_2^k \cdots x_m^s$$

or, finally,

$$\Phi(ux_1, \ldots, ux_m) = u^n \Phi(x_1, x_2, \ldots, x_m). \qquad (I)$$

A polynomial has this property precisely if it is a form, which can be seen by decomposing it into its homogeneous parts. It can consequently be used as a defining property of forms.

If we differentiate (I) with respect to u, which is admissible since it holds identically as an equation in u, then it follows that

$$\begin{aligned}&\frac{\partial\Phi(ux_1, \ldots)}{\partial(ux_1)} x_1 + \frac{\partial\Phi(ux_1, \ldots)}{\partial(ux_2)} x_2 + \cdots + \frac{\partial\Phi(ux_1, \ldots)}{\partial(ux_m)} x_m \\ &\quad = nu^{n-1}\Phi(x_1, \ldots),\end{aligned}$$

and if we set $u = 1$, then we obtain

$$x_1 \frac{\partial\Phi}{\partial x_1} + x_2 \frac{\partial\Phi}{\partial x_2} + \cdots + x_m \frac{\partial\Phi}{\partial x_m} = n\Phi. \qquad (II)$$

Lecture II (April 29, 1897)

There are two ways in which one can classify forms: either according to order or according to the number of variables—which is more commonly done. In the latter case there are special names for forms with a small number of variables:

1. $m = 1$. *Unary forms.* The general form is cx_1^n.
2. $m = 2$. *Binary forms.* Here the general expression is
$$\mathcal{F} = c_0 x_1^n + c_1 x_1^{n-1} x_2 + \cdots + c_n x_2^n.$$
The number of terms is $n + 1$.
3. $m = 3$. *Ternary forms.*
4. $m = 4$. *Quaternary forms.*
5. $m = 5$. *Quinary forms.*
6. $m = 6$. *Senary forms.*

The terminology for $m = 1, 5, 6$ is little used however. As the primary purpose of this section we are left with the *determination of the number of terms of a general form.* Let $\phi(n, m)$ be the number of terms of a general form of order n with m variables. We know—and it is easily seen—that
$$\phi(n, 2) = n + 1,$$
$$\phi(1, m) = m.$$
We claim now that the desired formula is
$$\phi(n, m) = \frac{(n+1)(n+2)(n+3)\cdots(n+m-1)}{1 \cdot 2 \cdot 3 \cdots (m-1)}. \qquad (III)$$
This formula is valid for $m = 2$. We will prove it for general m by induction from $m - 1$ to m. For this purpose we will use a recursion formula which can be derived as follows. Let $\mathcal{F}^{(n)}$ denote a form of order n; then in the general case we have the expression
$$\mathcal{F}^{(n)}(x_1, \ldots, x_m) = x_m^n \mathcal{F}^{(0)}(x_1, \ldots, x_{m-1}) + x_m^{n-1} \mathcal{F}^{(1)}(x_1, \ldots, x_{m-1}) + \cdots + x_m^0 \mathcal{F}^{(n)}(x_1, \ldots, x_{m-1}).$$
Therefore
$$\phi(n, m) = \phi(0, m-1) + \phi(1, m-1) + \cdots + \phi(n, m-1),$$

and, likewise,

$$\phi(n-1,m) = \phi(0,m-1) + \phi(1,m-1) + \cdots + \phi(n-1,m-1).$$

Subtraction of the two formulas results in

$$\phi(n,m) - \phi(n-1,m) = \phi(n,m-1)$$

or

$$\phi(n,m) = \phi(n-1,m) + \phi(n,m-1).$$

If we now set

$$\chi(n,m) = \phi(n,m) - \frac{(n+1)\cdots(n+m-1)}{1\cdot 2\cdot 3\cdots(m-1)},$$

then we obtain

$$\begin{aligned}\chi(n,m) - \chi(n-1,m) &= \phi(n,m) - \phi(n-1,m) \\ &\quad - \frac{(n+1)\cdots(n+m-1)}{1\cdot 2\cdots(m-1)} \\ &\quad + \frac{n(n+1)\cdots(n+m-2)}{1\cdot 2\cdots(m-1)} \\ &= \phi(n,m-1) - \frac{(n+1)(n+2)\cdots(n+m-2)}{1\cdot 2\cdots(m-2)} \\ &= 0,\end{aligned}$$

since we assume the formula to hold for $m-1$. Consequently,

$$\chi(n,m) = \chi(n-1,m) = \cdots = \chi(1,m),$$

through repeated application of the last formula. Hence, we obtain that

$$\chi(n,m) = \phi(1,m) - \frac{2\cdot 3\cdots m}{2\cdot 3\cdots(m-1)} = m - m = 0.$$

Therefore, formula (III) is valid for m variables, and is thus valid in general.

Lecture III (April 30, 1897)

Finally, we want to point out briefly a geometrical interpretation of the theory of forms. If, given a binary form, we set $x_1 = x$, $x_2 = 1$ (which

does not change the essential nature of the form, due to its homogeneity), then we obtain a polynomial in one variable of order n:

$$c_0x^n + c_1x^{n-1} + c_2x^{n-2} + \cdots + c_n.$$

The theory of binary forms therefore includes the theory of algebraic equations in one variable. If we interpret x_1, x_2 as the coordinates of a point on a line, then a binary form set equal to zero represents n points on a line. The theory of binary forms is thus also identical with the geometry of a line (or a bundle of lines and planes). Analogously, one realizes that a ternary form set equal to zero describes a relationship between two variables; hence the theory of ternary forms is identical to the geometry of the plane, namely, of algebraic curves. Finally, the theory of quaternary forms is analogously an essential aid in studying the geometry of space, especially of algebraic surfaces. The forms with more than three variables do not readily admit such a geometric interpretation.

I.2 The linear transformation

We are led to essentially new and deep properties of forms through the application of linear transformations. Let

$$\mathcal{F}^{(n)}(x_1, x_2, \ldots, x_m)$$

be a general form. We can derive another form from it, if we replace the m variables x by other variables x' via relations of the form

$$\begin{aligned} x_1 &= \phi_1(x'_1, \ldots, x'_m), \\ x_2 &= \phi_2(x'_1, \ldots, x'_m), \\ &\cdots \\ x_m &= \phi_m(x'_1, \ldots, x'_m), \end{aligned}$$

where the ϕs denote forms of the same order. Such an operation is called a *transformation*, the new variables are called x', and the resulting form

$$\begin{aligned} &\mathcal{F}'(x'_1, x'_2, \ldots, x'_m) \\ &\quad = \mathcal{F}(\phi_1(x'_1, \ldots, x'_m), \phi_2(x'_1, \ldots, x'_m), \ldots, \phi_m(x'_1, \ldots, x'_m)) \end{aligned}$$

is called the *transformed form.*

Among the transformations, the linear ones are distinguished, that is, the transformations for which $\phi_1, \phi_2, \ldots, \phi_m$ are linear forms. The

relationship is then given by the following equations—here again we want to fix notation:

$$\begin{aligned} x_1 &= \alpha_{11}x'_1 + \alpha_{12}x'_2 + \cdots + \alpha_{1m}x'_m, \\ x_2 &= \alpha_{21}x'_1 + \alpha_{22}x'_2 + \cdots + \alpha_{2m}x'_m, \\ &\cdots \\ x_m &= \alpha_{m1}x'_1 + \alpha_{m2}x'_2 + \cdots + \alpha_{mm}x'_m. \end{aligned}$$

The α are called the *transformation coefficients*. We regard them as given, without ever specifying them. The transformed form becomes

$$\begin{aligned} \mathcal{F}'(x'_1, x'_2, \ldots, x'_m) &= \mathcal{F}(x_1, x_2, \ldots, x_m) \\ &= \mathcal{F}(\alpha_{11}x'_1 + \cdots, \ldots, \alpha_{m1}x'_1 + \cdots). \end{aligned}$$

Here, we primarily need to observe three properties of linear transformations:

1. The transformed form has the same order as the original form. This is because the general term

$$c_i x_1^{\nu_1} x_2^{\nu_2} \cdots x_m^{\nu_m}, \qquad \nu_1 + \nu_2 + \cdots + \nu_m = n,$$

becomes

$$c_i(\alpha_{11}x'_1 + \alpha_{12}x'_2 + \cdots)^{\nu_1}(\alpha_{21}x'_1 + \cdots)^{\nu_2} \cdots (\alpha_{m1}x'_1 + \cdots)^{\nu_m},$$

from which it is apparent that in each new term the coefficients c_i appear homogeneously to the first power, the transformation coefficients α appear homogeneously to the nth power, and the variables x' also appear homogeneously to the nth power. We now want to write the transformed form exactly like the original one, only with primed letters, namely:

$$\mathcal{F}(x_1, x_2, \ldots, x_m) = c_0x_1^n + c_1x_1^{n-1}x_2 + c_2x_1^{n-2}x_2^2 + c_3x_1^{n-1}x_3 + \cdots$$

equals

$$\mathcal{F}'(x'_1, x'_2, \ldots, x'_m) = c'_0{x'_1}^n + c'_1{x'_1}^{n-1}x'_2 + c'_2{x'_1}^{n-2}{x'_2}^2 + c'_3{x'_1}^{n-1}x'_3 + \cdots .$$

Observe that not only is the stated theorem valid, but we have also shown that the new coefficients c'_i are homogeneous functions of degree one of the original coefficients, and homogeneous functions of degree n of the transformation coefficients α.

A simple example might serve as an illustration.

Let

$$\mathcal{F}^{(2)}(x_1, x_2) = Ax_1^2 + Bx_1x_2 + Cx_2^2.$$

Using the transformation

$$x_1 = \alpha_{11}x'_1 + \alpha_{12}x'_2,$$
$$x_2 = \alpha_{21}x'_1 + \alpha_{22}x'_2,$$

we obtain

$$\mathcal{F} = A'x'^2_1 + B'x'_1x'_2 + C'x'^2_2 = \mathcal{F}'^{(2)}(x'_1, x'_2),$$

where

$$A' = A\alpha^2_{11} + B\alpha_{11}\alpha_{21} + C\alpha^2_{21},$$
$$B' = 2A\alpha_{11}\alpha_{12} + B(\alpha_{11}\alpha_{22} + \alpha_{12}\alpha_{21}) + 2C\alpha_{21}\alpha_{22},$$
$$C' = A\alpha^2_{12} + B\alpha_{12}\alpha_{22} + C\alpha^2_{22}.$$

This confirms the assertions made above.

2. The transformation is invertible. Indeed, to recover the original form from the transformed one, we only need to solve the above equations for the x', which is possible since there are m equations for the m variables x'. We only need to assume—and we want to keep this assumption; it is the only one we need to make—that the *transformation determinant*, that is, the determinant of the transformation coefficients

$$A = \begin{vmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1m} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2m} \\ & & \cdots & \\ \alpha_{m1} & \alpha_{m2} & \cdots & \alpha_{mm} \end{vmatrix},$$

is different from zero. If the $(m-1)\times(m-1)$ minors of this determinant are A_{ik}, then the solved equations are

$$Ax'_1 = A_{11}x_1 + A_{21}x_2 + \cdots + A_{m1}x_m,$$
$$Ax'_2 = A_{12}x_1 + A_{22}x_2 + \cdots + A_{m2}x_m,$$
$$\cdots$$
$$Ax'_m = A_{1m}x_1 + A_{2m}x_2 + \cdots + A_{mm}x_m.$$

The pattern is very easy to surmise; compared to the other equations the indices are simply transposed. We have

$$x_i = \alpha_{i1}x'_1 + \alpha_{i2}x'_2 + \cdots + \alpha_{im}x'_m,$$
$$Ax'_i = A_{1i}x_1 + A_{2i}x_2 + \cdots + A_{mi}x_m.$$

Lecture IV (May 3, 1897)

3. The group property of linear transformations. If we first apply the transformation

$$x_1 = \alpha_{11}x'_1 + \alpha_{12}x'_2 + \cdots + \alpha_{1m}x'_m,$$
$$\cdots$$
$$x_m = \alpha_{m1}x'_1 + \alpha_{m2}x'_2 + \cdots + \alpha_{mm}x'_m$$

to a form $\mathcal{F}$, then we obtain the transformed form $\mathcal{F}'^{(n)}(x'_1, x'_2)$. To this form we now want to apply a second linear transformation, such as

$$x'_1 = \beta_{11}x''_1 + \beta_{12}x''_2 + \cdots + \beta_{1m}x''_m,$$
$$\cdots$$
$$x'_1 = \beta_{m1}x''_1 + \beta_{m2}x''_2 + \cdots + \beta_{mm}x''_m.$$

In this way we obtain a new form $\mathcal{F}''^{(n)}(x''_1, x''_2)$. The order of this form is the same as that of the original form. It is now clear that one can replace the two steps by a single one, since one has

$$\begin{aligned} x_i = {} & \alpha_{i1}(\beta_{11}x''_1 + \beta_{12}x''_2 + \cdots + \beta_{1m}x''_m) \\ & + \alpha_{i2}(\beta_{21}x''_1 + \beta_{22}x''_2 + \cdots + \beta_{2m}x''_m) \\ & \cdots \\ & + \alpha_{im}(\beta_{m1}x''_1 + \beta_{m2}x''_2 + \cdots + \beta_{mm}x''_m). \end{aligned}$$

From this it is immediately clear that one can obtain the x'' from the x directly through *one* linear transformation, namely, through the following one:

$$x_1 = \gamma_{11}x''_1 + \gamma_{12}x''_2 + \cdots + \gamma_{1m}x''_m,$$
$$\cdots$$
$$x_m = \gamma_{m1}x''_1 + \gamma_{m2}x''_2 + \cdots + \gamma_{mm}x''_m,$$

where we set

$$\gamma_{il} = \alpha_{i1}\beta_{1l} + \alpha_{i2}\beta_{2l} + \cdots + \alpha_{ik}\beta_{kl} + \cdots + \alpha_{im}\beta_{ml}\ .$$