

15. The Finiteness of the System of Integral Invariants of Binary Forms

15. The Finiteness of the System of Integral Invariants of Binary Forms

Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen 1919, pp. 138–156

By

Emmy Noether in Göttingen.

Presented by F. Klein in the session of 27 March 1919.

In what follows, as an extension of the known finiteness theorem, the following theorem is proved: *All polynomial integral invariants of a binary system of ground forms are polynomial rational functions, with integral coefficients, of a finite number among them.* Here, as usual, by an “invariant” one always means a polynomial rational invariant of a ground form or of a system of ground forms, namely an invariant with respect to the coefficient transformation induced by the group of all linear transformations.

The proof rests on an integrality sharpening of the Mertens-Hilbert proof of finiteness.⁵³ This proof of finiteness may be characterized as follows. One decomposes the ground forms into their linear factors - more precisely, one associates to each ground form a product of linear forms - whereby each invariant I is changed into an invariant of these linear forms, hence into a function of the homogenized roots. This function has to satisfy three conditions: 1) the condition of invariance, 2) weight conditions, and 3) symmetry conditions. Conditions 2) and 3) are necessary for I to become polynomial and rational in the coefficients of the ground forms. Condition 1) is satisfied by representing I as a polynomial rational function of the determinants of the linear forms; condition 2) by taking, instead of the individual determinants, certain products of powers of them as new arguments. Condition 3) then simply says that I becomes a polynomial rational symmetric function of rows of quantities, and that conversely every such symmetric function of rows of quantities becomes an invariant of the ground forms. The elementary symmetric functions of these rows of quantities therefore give the complete system.

If one considers only integral invariants, condition 1) can be satisfied just as above as soon as, for invariants of linear forms, the sharper theorem is proved that *all integral invariants of binary linear forms are polynomial integral functions of the determinants of these linear forms.* I show that this is in fact the case in § 3, in the form that the totality of all relations modulo any prime between these determinants coincides with the totality of all identical relations; that is, the module corresponding to these relations remains a prime module modulo every prime number. This verification is carried out by normalizing the residue classes with respect to the module of quadratic forms corresponding to the quadratic relations between the determinants; these quadratic forms thereby turn out to form an integral basis of the module, modulo every prime, whereas previously they were known as a module basis only when integrality was disregarded.

To satisfy condition 2) no alteration is needed, since the introduction of products of powers does not affect the integer coefficients. Condition 3) now says that $n_1! \cdots n_\mu! I$ (where $n_1, \dots, n_\mu$ are the degrees of the individual ground forms) becomes an integral symmetric function of rows of quantities, and conversely every integral symmetric function of these rows becomes an integral invariant. But, as is easily shown, these integral symmetric functions of rows possess an integral basis, for which the elementary functions alone no longer suffice. The application of Hilbert’s theorem on the integral module basis then also yields an integral basis for the I themselves.

Section 1 collects the special finiteness theorems corresponding to conditions 1), 2), and 3), from which the proof of finiteness follows in § 2. The special finiteness theorems corresponding to condition 3) also yield the finiteness of the integral invariants of finite groups of integral or algebraic-integral substitutions, as is briefly carried out in § 4.

⁵³F. Mertens, Wiener Sitzungsberichte Jan. 1889; D. Hilbert, *Math. Ann.* vol. 33 (1889) [dated March 1888]. The two proofs, which arose independently of one another following Mertens, Crelle vol. 100, agree in content.

§ 1. Special Finiteness Theorems

I first state the following special finiteness theorems, which will serve to satisfy the conditions of invariance, weight, and symmetry mentioned in the introduction.

I. Every integral invariant of a system of binary linear forms is a polynomial rational function, with integral coefficients, of the determinants of these linear forms. The proof will be given in § 3.

II. Every system $\mathfrak{S}$ of products of powers of n variables with nonnegative exponents, which together with any two products of powers f and g also contains their quotient whenever this quotient is polynomial in the variables, has a finite multiplicative basis $f_1, \dots, f_k$ consisting of functions from $\mathfrak{S}$, such that for every f in $\mathfrak{S}$ one has a representation

$$f = f_1^{\lambda_1} \cdots f_k^{\lambda_k}$$

with nonnegative exponents $\lambda_1, \dots, \lambda_k$.

Indeed, by Hilbert's theorem on the module basis there exists a finite number of functions from $\mathfrak{S}$, say $f_1, \dots, f_k$, each of which really contains the x 's, such that every nonconstant f from $\mathfrak{S}$ belongs to the module generated by them:

$$f \equiv 0 \pmod{(f_1, \dots, f_k)}.$$

It follows that for every $f = x_1^{i_1} \cdots x_n^{i_n}$ there is at least one $f_\nu = x_1^{\nu_1} \cdots x_n^{\nu_n}$ such that $\nu_1 \leq i_1, \dots, \nu_n \leq i_n$. In the representation

$$f = x_1^{i_1 - \nu_1} \cdots x_n^{i_n - \nu_n} f_\nu = A f_\nu$$

the factor A belongs to $\mathfrak{S}$ by hypothesis, but it has lower degree in the variables than f . Hence by repeating the argument finitely many times the assertion follows. In order that the representation also hold for $f = 1$, one need only put all exponents λ equal to zero.⁵⁴

III. All polynomial integral symmetric functions of n rows of quantities are polynomial integral functions of a finite number among them.

Let $\tau_1(x), \dots, \tau_n(x)$ denote the elementary symmetric functions of the indeterminates $x_1, \dots, x_n$. Then for every exponent k there is an identity

$$x_i^k = G_0^{(k)}(\tau) + x_i G_1^{(k)}(\tau) + \cdots + x_i^{n-1} G_{n-1}^{(k)}(\tau), \quad (i = 1, 2, \dots, n),$$

where $G_0^{(k)}, \dots, G_{n-1}^{(k)}$ are polynomial integral functions of the $\tau(x)$. If $x_i, y_i, \dots, z_i$ are the elements of the i -th row, then by these identities and the corresponding ones for $y, \dots, z$, all special, one-rowed symmetric functions

$$\sum_{i=1}^n x_i^a y_i^b \cdots z_i^c$$

become polynomial integral functions of the finitely many

$$\sum_{i=1}^n x_i^a y_i^b \cdots z_i^c \quad (0 \leq a < n, 0 \leq b < n, \dots, 0 \leq c < n)$$

and of the elementary symmetric functions $\tau(x), \tau(y), \dots, \tau(z)$.⁵⁵ If one has the most general symmetric functions of the n rows - a case not occurring below - it is shown in the same way that the functions

$$\sum x_{i_1}^{a_1} y_{i_1}^{b_1} \cdots z_{i_1}^{c_1} x_{i_2}^{a_2} y_{i_2}^{b_2} \cdots z_{i_2}^{c_2} \cdots x_{i_n}^{a_n} y_{i_n}^{b_n} \cdots z_{i_n}^{c_n} \\ (0 \leq a_\nu < n, 0 \leq b_\nu < n, \dots, 0 \leq c_\nu < n),$$

where $i_1, i_2, \dots, i_n$ runs through all permutations, together with $\tau(x), \tau(y), \dots, \tau(z)$, form an integral basis.

IV. Let $F_1(x), \dots, F_k(x)$ be polynomial integral functions of $x_1, \dots, x_n$, and let a be a fixed integer. Then all functions

$$\frac{G(F)}{a},$$

⁵⁴This representation can also be proved directly, and conversely Hilbert's theorem follows from it: compare P. Gordan, Neuer Beweis des Hilbertschen Satzes über homogene Funktionen, Gött. Nachr. 1899. Another direct proof of this representation, from which Theorem II is also derived, is in A. Ostrowski, Über die Existenz einer endlichen Basis bei gewissen Funktionensystemen, Math. Ann. 78 (1916), § 2,1 and § 3,2. The special case of Theorem II used in § 2, where the exponents run through all nonnegative solutions of a Diophantine system of equations, is already found in Gordan-Kerschensteiner, Vorlesungen über Invariantentheorie, vol. I, p. 199.

⁵⁵Hilbert, loc. cit., takes the power sums instead of the $\tau(x), \dots, \tau(z)$ into the basis; this makes the basis consist only of one-rowed functions, but the integrality of the representation is then lost.

where G denotes a polynomial integral function, which become integral in the x 's, are polynomial integral functions of a finite number among them.

Indeed, by Hilbert's theorem on the integral module basis, for each such $G(F)/a$ one has a representation

$$\frac{G(F)}{a} = A_1(F_1 \dots F_k) \frac{G_1(F)}{a} + \dots + A_\rho(F_1 \dots F_k) \frac{G_\rho(F)}{a},$$

where $A_1, \dots, A_\rho$ are polynomial integral functions of the F 's, and

$$\frac{G_1(F)}{a}, \dots, \frac{G_\rho(F)}{a}$$

belong to the system. The functions

$$F_1 = \frac{aF_1}{a}, \dots, F_k = \frac{aF_k}{a}; \quad \frac{G_1(F)}{a}, \dots, \frac{G_\rho(F)}{a}$$

therefore form the required basis.

§ 2. Finiteness of the Integral Binary Invariants

Let x, y be binary variables subjected to a transformation with indeterminate coefficients

$$x = s_{11}x' + s_{12}y', \quad y = s_{21}x' + s_{22}y', \quad (1)$$

and let f be a binary ground form whose coefficients are indeterminates. Then by (1),

$$f = a_0x^n + a_1x^{n-1}y + \dots + a_ny^n = a'_0x'^n + a'_1x'^{n-1}y' + \dots + a'_ny'^n. \quad (2)$$

By an integral invariant of f one understands, as is well known, a polynomial integral function $I(a)$ such that

$$I(a') = |s_{ik}|^\rho I(a), \quad \text{identically in } a, s_{ik}. \quad (3)$$

The integral invariants of a system of ground forms are defined correspondingly; one may include homogeneity in the coefficients of the individual ground forms in the definition, since from such individually homogeneous invariants the remaining ones are composed in an integral-linear way.

In addition to (2), consider a special binary form g , namely the product of n linear forms whose coefficients are again indeterminates:⁵⁶

$$\begin{aligned} g &= (\alpha_1x + \beta_1y)(\alpha_2x + \beta_2y) \dots (\alpha_nx + \beta_ny) \\ &= \sigma_0(\alpha, \beta)x^n + \sigma_1(\alpha, \beta)x^{n-1}y + \dots + \sigma_n(\alpha, \beta)y^n \\ &= (\alpha'_1x' + \beta'_1y')(\alpha'_2x' + \beta'_2y') \dots (\alpha'_nx' + \beta'_ny') \\ &= \sigma'_0x'^n + \sigma'_1x'^{n-1}y' + \dots + \sigma'_ny'^n. \end{aligned} \quad (4)$$

Thus $\sigma_0(\alpha, \beta), \sigma_1(\alpha, \beta), \dots, \sigma_n(\alpha, \beta)$ denote the homogenized elementary symmetric functions, and the transformed coefficients σ'_i become equal to $\sigma_i(\alpha', \beta')$.

Because of the algebraic independence of these elementary functions, to every relation

$$G(\sigma_0, \sigma_1, \dots, \sigma_n) = 0 \quad \text{identically in } \alpha, \beta \quad (5)$$

there corresponds a further relation

$$G(\sigma_0, \sigma_1, \dots, \sigma_n) = 0 \quad \text{identically in } \sigma_0, \dots, \sigma_n, \quad (6)$$

and hence, for indeterminates $a_0, \dots, a_n$,

$$G(a_0, a_1, \dots, a_n) = 0 \quad \text{identically in } a_0, \dots, a_n. \quad (7)$$

⁵⁶If, as is often done in invariant theory, one writes f with binomial coefficients, $f = b_0x^n + \binom{n}{1}b_1x^{n-1}y + \dots + b_ny^n$, then the domain of all integral invariants $I(b)$ is enlarged relative to that of the $I(a)$, and the finiteness arguments used here fail; $I(b)$ is no longer an integral function of the roots.

Now every integral invariant $I(a)$ of f , by the substitution $a_i = \sigma_i(\alpha, \beta)$, gives an integral invariant $I(\sigma) = H(\alpha, \beta)$ of g , where H becomes an integral function of α, β . For this invariant the relation (3) becomes

$$I(\sigma') = |s_{ik}|^\rho I(\sigma) \quad \text{identically in } \sigma, s_{ik}, \quad (8)$$

and since $\sigma' = \sigma(\alpha', \beta')$, (8) gives

$$H(\alpha', \beta') = |s_{ik}|^\rho H(\alpha, \beta) \quad \text{identically in } \alpha, \beta; s_{ik}. \quad (9)$$

Thus $I(\sigma) = H(\alpha, \beta)$ becomes an integral invariant of the n linear forms $(\alpha_i x + \beta_i y)$. Conversely, suppose $H(\alpha, \beta)$ is an integral invariant of these n linear forms, hence satisfies (9), and is at the same time equal to an integral function $I(\sigma)$ of the σ 's. Since then

$$H(\alpha', \beta') = I(\sigma(\alpha', \beta')) = I(\sigma'),$$

equation (9) can also be written

$$I(\sigma') = |s_{ik}|^\rho I(\sigma) \quad \text{identically in } \alpha, \beta; s_{ik}. \quad (9a)$$

It follows from (5) and (6) that (8) holds, and from (7) that (3) holds. Therefore to every integral invariant $I(a)$ there corresponds an integral invariant $H(\alpha, \beta) = I(\sigma)$ of the n linear forms, and conversely. Moreover, if $I_1(a), \dots, I_k(a)$ is an integral basis of all $I(a)$, then $H_1(\alpha, \beta), \dots, H_k(\alpha, \beta)$ is an integral basis of all $H(\alpha, \beta)$ which are at the same time integral functions $I(\sigma)$; here too the converse holds by (5), (6), and (7). Thus, to prove the existence of an integral basis for all $I(a)$, it suffices to prove it for all integral invariants $H(\alpha, \beta)$ which are at the same time integral functions $I(\sigma)$; and the basis

$$H_1(\alpha, \beta) = I_1(\sigma), \dots, H_k(\alpha, \beta) = I_k(\sigma)$$

then supplies the basis $I_1(a), \dots, I_k(a)$ for the $I(a)$.

Let $H(\alpha, \beta) = I(\sigma)$ run through the totality of all integral invariants of (4). Since by (3) every invariant is homogeneous in the σ 's, and by (4) each σ is homogeneous and linear in the coefficients of each linear form, $H(\alpha, \beta)$ is homogeneous in each row α_i, β_i and of the same dimension in each row; moreover it is of course a symmetric function of the n rows. Conversely, by the fundamental theorem on symmetric functions, every integral symmetric function $H(\alpha, \beta)$ of the n rows, homogeneous separately and of the same dimension in each row, is a polynomial integral function of the σ 's. Thus, by the preceding argument, it is an invariant $I(\sigma)$ as soon as $H(\alpha, \beta)$ is invariant. The totality of the integral invariants of (4) is therefore characterized as the totality of integral functions $H(\alpha, \beta)$ with the following properties:

- 1) integral invariant of the n linear forms $\alpha_i x + \beta_i y$;
- 2) separately homogeneous and of the same dimension in each of the n rows α_i, β_i ;
- 3) symmetric in the n rows α_i, β_i .

By the special finiteness theorem I, $H(\alpha, \beta)$, because of 1), becomes a polynomial integral function of the determinants

$$(ik) = \alpha_i \beta_k - \beta_i \alpha_k;$$

hence

$$H(\alpha, \beta) = G((ik)).$$

In this representation the symmetry can also be expressed formally by applying all permutations of the n rows to $G((ik))$:

$$n! H(\alpha, \beta) = G^{(1)}((ik)) + G^{(2)}((ik)) + \dots + G^{(n!)}((ik)) = G^*((ik)). \quad (10)$$

Along with each product of powers P of the (ik) , G^* therefore also contains the sum $Q = P^{(1)} + \dots + P^{(n!)}$ over all permutations of P . In fact G^* becomes an integral linear combination of finitely many Q 's, $G^* = \sum cQ$. Since the Q 's satisfy conditions 1), 2), and 3), and hence themselves become invariants, it suffices to consider the Q 's in place of $G^*((ik))$.

Now let P run through the system $\mathfrak{S}$ of all products of powers of the (ik) occurring in the Q 's, i.e. satisfying condition 2). If the quotient of two P 's is polynomial in the (ik) , then it also satisfies condition

2), and hence belongs to $\mathfrak{S}$. Therefore, by Theorem II, there are finitely many such P 's, say $P_1, \dots, P_\rho$, such that every P is representable in the form

$$P = P_1^{\lambda_1} \dots P_\rho^{\lambda_\rho}$$

with nonnegative exponents λ . Applying all permutations gives

$$Q = P_1^{(1)\lambda_1} \dots P_\rho^{(1)\lambda_\rho} + \dots + P_1^{(n!)\lambda_1} \dots P_\rho^{(n!)\lambda_\rho}.$$

Thus Q becomes an integral symmetric function of the $n!$ rows of quantities, each with ρ elements:

$$P_1^{(1)} \dots P_\rho^{(1)}; \quad P_1^{(2)} \dots P_\rho^{(2)}; \quad \dots; \quad P_1^{(n!)} \dots P_\rho^{(n!)};$$

hence, by Theorem III, it is a polynomial integral function of finitely many symmetric functions of these rows. These basis functions are themselves quantities Q or elementary symmetric functions of the $n!$ elements $P_i^{(1)}, P_i^{(2)}, \dots, P_i^{(n!)}$, and therefore satisfy conditions 1), 2), and 3) and become integral invariants

$$H_1(\alpha, \beta) = I_1(\sigma); \dots; \quad H_l(\alpha, \beta) = I_l(\sigma). \quad (11)$$

By (10), since $G^* = \sum cQ$, every $H(\alpha, \beta) = I(\sigma)$ is therefore of the form

$$H(\alpha, \beta) = I(\sigma) = \frac{1}{n!} \Phi(I_1, \dots, I_l),$$

where Φ denotes a polynomial integral function; conversely, $\frac{1}{n!} \Phi$ is an integral invariant as soon as it is polynomial in α, β . Hence by Theorem IV finitely many further invariants $I_{l+1}(\sigma), \dots, I_k(\sigma)$ can be adjoined to (11) in such a way that

$$\begin{aligned} H_1(\alpha, \beta) &= I_1(\sigma); \dots; H_l(\alpha, \beta) = I_l(\sigma); \\ H_{l+1}(\alpha, \beta) &= I_{l+1}(\sigma); \dots; H_k(\alpha, \beta) = I_k(\sigma) \end{aligned}$$

form an integral basis of all invariants $H(\alpha, \beta) = I(\sigma)$. This proves the theorem for the case of one ground form.

If one is dealing with a system of ground forms, then, as noted above, one may assume homogeneity of the invariants in the coefficients of each ground form. One again replaces the general ground forms by ones which are respectively products of linear forms. Their invariants then become: 1) invariants of these linear forms; 2) separately homogeneous in the rows formed from the coefficients of the linear forms, and of equal dimension in the rows belonging to each individual ground form; 3) symmetric in the rows belonging to each individual ground form. Conversely, each integral invariant of all the linear forms satisfying these conditions again corresponds to an integral invariant of the system of ground forms. The proof is absolutely parallel to that just given. To each product of powers $P = P_1^{\lambda_1} \dots P_\rho^{\lambda_\rho}$ of the individual determinants satisfying the weight conditions (Theorems I and II) one must apply all

$$N = n_1! n_2! \dots n_\mu!$$

permutations, where $n_1, \dots, n_\mu$ denote the degrees of the ground forms. In this way $N \cdot I$ is converted into an integral symmetric function of N rows, each with ρ elements. From this one obtains the integral basis for all $N \cdot I$, and consequently, by Theorem IV, the integral basis for all I .

§ 3. The Basis of the Integral Invariants of Binary Linear Forms

It remains to supply the proof of the special finiteness theorem I. By a known theorem, first proved by Clebsch, all polynomial rational invariants of the n linear forms $\alpha_i x + \beta_i y$ are polynomial rational functions of the determinants (ik) . In particular, therefore, all integral invariants of these linear forms become polynomial rational, though not necessarily integral, functions of these determinants.

It will be shown below that, in view of the identical relations existing between the (ik) , this representation is always possible integrally.

In formulas, and in the language of module theory, this is expressed as follows. Let ξ_{ik} , $i < k$, be indeterminates. Then the totality of all integral polynomials $F(\xi_{ik})$ with the property that $F((ik))$ vanishes

identically in α, β forms a module $\mathfrak{M}$; the sum of two such F 's, and also the product of such an F with an arbitrary integral polynomial in the ξ_{ik} , again belongs to this totality. In formulas:

$$F((ik)) = 0 \quad \text{identically in } \alpha, \beta$$

implies

$$F(\xi_{ik}) \equiv 0 \pmod{\mathfrak{M}} \quad \text{identically in } \xi_{ik},$$

and conversely.

I now show that the following completely analogous statement holds. From

$$F((ik)) \equiv 0 \pmod{p} \quad \text{identically in } \alpha, \beta$$

$$\text{it follows that} \quad F(\xi_{ik}) \equiv 0 \pmod{(\mathfrak{M}, p)} \quad \text{identically in } \xi_{ik}, \quad (1)$$

and conversely, for every prime number p . Hence $\mathfrak{M}$ is also identical with the module $\mathfrak{M}_p$ corresponding to the totality of all relations modulo p among the (ik) ; this module consists of all integral polynomials $F(\xi_{ik})$ for which $F((ik))$ vanishes identically modulo p in α, β .

That (1) asserts the integral representability is seen as follows. It can also be written in the form: from $F((ik)) = p \cdot H(\alpha, \beta)$, identically in α, β , it follows that

$$F(\xi_{ik}) - p \cdot G(\xi_{ik}) \equiv 0 \pmod{\mathfrak{M}} \quad \text{identically in } \xi_{ik},$$

and hence, by the definition of $\mathfrak{M}$,

$$F((ik)) = p \cdot G((ik)) \quad \text{identically in } \alpha, \beta.^{57}$$

Thus $p \cdot H(\alpha, \beta) = p \cdot G((ik))$, or

$$H(\alpha, \beta) = G((ik)).$$

If, therefore, a representation is given

$$H(\alpha, \beta) = \frac{1}{p_1^{\lambda_1} \cdots p_\rho^{\lambda_\rho}} F((ik)),$$

where $p_1, \dots, p_\rho$ are prime numbers, then it follows also that

$$H(\alpha, \beta) = \frac{1}{p_1^{\lambda_1-1} \cdots p_\rho^{\lambda_\rho}} G((ik)),$$

and by repeating this finitely many times one obtains the integrality of the representation.

For the proof of (1), denote by

$$f_{ik,rs} = \xi_{ik}\xi_{rs} - \xi_{ir}\xi_{ks} + \xi_{is}\xi_{kr}, \quad i < k < r < s,$$

the forms in the indeterminates ξ_{ik} corresponding to the quadratic relations between the (ik) ,

$$(ik)(rs) - (ir)(ks) + (is)(kr) = 0,$$

and denote by $\mathfrak{N} = (f_{ik,rs})$ the module of integral polynomials generated from them. From

$$F(\xi_{ik}) \equiv 0 \pmod{\mathfrak{N}}$$

it follows that

$$F((ik)) = 0 \quad \text{identically in } \alpha, \beta,$$

and

$$\begin{aligned} \text{from } F(\xi_{ik}) &\equiv 0 \pmod{(\mathfrak{N}, p)} \\ \text{it follows that } F((ik)) &\equiv 0 \pmod{p} \quad \text{identically in } \alpha, \beta. \end{aligned} \quad (2)$$

I shall now show, by normalizing the residue classes with respect to $\mathfrak{N}$, that the converse of (2) also holds. Then $\mathfrak{N} = \mathfrak{M} = \mathfrak{M}_p$, and (1) will be proved. The equality $\mathfrak{N} = \mathfrak{M}$ is obtained as the special case $\mathfrak{N} = \mathfrak{M}_p$ for $p = 0$; the case $p = 0$ is always included in the following considerations. In other words, the $f_{ik,rs}$ form an integral module basis of $\mathfrak{M}_p$, and in particular also of $\mathfrak{M}_0 = \mathfrak{M}$.

⁵⁷This latter conclusion simultaneously proves the converse of (1).

a) The case of two or three rows α_i, β_i

Since no four different indices occur, $\mathfrak{N}$ is the zero module. It must therefore be shown that from

$$F((ik)) \equiv 0 \pmod{p} \quad \text{identically in } \alpha, \beta \quad (3)$$

it follows that

$$F(\xi_{ik}) \equiv 0 \pmod{p} \quad \text{identically in } \xi_{ik}.$$

This proves (1) with $\mathfrak{M} = \mathfrak{M}_p = 0$.

Since the condition $F((ik)) = p \cdot H(\alpha, \beta)$ must be satisfied separately by the components homogeneous in the individual rows, it is enough throughout to assume $F((ik))$ homogeneous in each individual row, and hence $F(\xi_{ik})$ homogeneous in each index. In the case of two rows there is only the one determinant (12) and the corresponding indeterminate ξ_{12} . By the assumed homogeneity,

$$F = c \xi_{12}^\nu.$$

From

$$c(12)^\nu \equiv 0 \pmod{p} \quad \text{identically in } \alpha, \beta$$

it follows, since $(12) \not\equiv 0 \pmod{p}$ identically in α, β , that $c \equiv 0 \pmod{p}$; hence

$$F(\xi_{ik}) \equiv 0 \pmod{p} \quad \text{identically in } \xi_{ik}.$$

This proves (3), and hence (1).

In the case of three rows there are the determinants (12), (13), (23), corresponding to the indeterminates $\xi_{12}, \xi_{13}, \xi_{23}$. Thus

$$F = \sum c \xi_{12}^{\tau_{12}} \xi_{13}^{\tau_{13}} \xi_{23}^{\tau_{23}}.$$

Let F have respectively the degrees $\sigma_1, \sigma_2, \sigma_3$ in the indices 1, 2, 3. Then

$$\sigma_1 = \tau_{12} + \tau_{13}, \quad \sigma_2 = \tau_{12} + \tau_{23}, \quad \sigma_3 = \tau_{13} + \tau_{23},$$

with the unique inverse

$$\tau_{12} = \frac{1}{2}(\sigma_1 + \sigma_2 - \sigma_3), \quad \tau_{13} = \frac{1}{2}(\sigma_1 - \sigma_2 + \sigma_3), \quad \tau_{23} = \frac{1}{2}(-\sigma_1 + \sigma_2 + \sigma_3).$$

Thus each separately homogeneous F contains at most one term,

$$F = c \xi_{12}^{\tau_{12}} \xi_{13}^{\tau_{13}} \xi_{23}^{\tau_{23}},$$

from which, as above, (3), and consequently (1), follows.

b) The case of four rows α_i, β_i

The six indeterminates $\xi_{12}, \xi_{13}, \xi_{14}, \xi_{23}, \xi_{24}, \xi_{34}$, and the corresponding determinants, occur; and $\mathfrak{N} = (f_{12,34})$. Since

$$\xi_{14}\xi_{23} \equiv \xi_{13}\xi_{24} - \xi_{12}\xi_{34} \pmod{\mathfrak{N}}, \quad (4)$$

every product of powers of the ξ_{ik} is congruent modulo $\mathfrak{N}$ to an integral linear combination of such products of powers in which the product $\xi_{14}\xi_{23}$ does not occur. Thus for every polynomial $F(\xi_{ik})$,

$$F(\xi_{ik}) \equiv F_0(\xi_{ik}) \pmod{\mathfrak{N}}, \quad (5)$$

where F_0 contains no product $\xi_{14}\xi_{23}$. The polynomial F_0 will be called the normalized polynomial of the residue class of F . Since (4) is separately homogeneous, a separately homogeneous F again corresponds to a separately homogeneous F_0 .

Now put

$$F_0(\xi_{ik}) = G(\xi_{ik}) + \xi_{34}F_1(\xi_{ik}), \quad (6)$$

where G contains no product of powers divisible by ξ_{34} , and further put

$$[G]_{\xi_{14}=\xi_{13}} = K(\xi_{12}, \xi_{13}, \xi_{23}). \quad (7)$$

From

$$F((ik)) \equiv 0 \pmod{p} \quad \text{identically in } \alpha, \beta$$

it follows by (5), taking account of (2), that

$$F_0((ik)) \equiv 0 \pmod{p} \quad \text{identically in } \alpha, \beta. \quad (8)$$

By specializing $\alpha_4 = \alpha_3$, $\beta_4 = \beta_3$, (6) and (7) give

$$K((ik)) \equiv 0 \pmod{p} \quad \text{identically in } \alpha, \beta.$$

By the result proved under a), therefore,

$$K(\xi_{ik}) \equiv 0 \pmod{p} \quad \text{identically in } \xi_{ik}.$$

From this follows what remains to be shown below:

$$G(\xi_{ik}) \equiv 0 \pmod{p} \quad \text{identically in } \xi_{ik}.$$

Thus (6) gives

$$F_0(\xi_{ik}) \equiv \xi_{34} F_1(\xi_{ik}) \pmod{p} \quad \text{identically in } \xi_{ik}.$$

Since (34) $\not\equiv 0 \pmod{p}$ identically in α, β , it follows from (8) that

$$F_1((ik)) \equiv 0 \pmod{p} \quad \text{identically in } \alpha, \beta,$$

where $F_1(\xi_{ik})$ is again normalized and of lower degree in ξ_{34} . Repeating the procedure finitely many times yields

$$F_0(\xi_{ik}) \equiv \xi_{34}^\lambda F_\lambda(\xi_{ik}) \pmod{p},$$

where F_λ is of degree zero in ξ_{34} , and hence vanishes modulo p by what has just been proved. Therefore

$$\begin{aligned} F_0(\xi_{ik}) &\equiv 0 \pmod{p} \quad \text{identically in } \xi_{ik}, \quad \text{or} \\ F(\xi_{ik}) &\equiv 0 \pmod{(\mathfrak{N}, p)} \quad \text{identically in } \xi_{ik}. \end{aligned} \quad (9)$$

This proves the converse of (2), and hence (1), at the same time in the sharper assertion for $F_0(\xi_{ik})$.⁵⁸

It remains only to add that $G(\xi_{ik}) \equiv 0 \pmod{p}$ follows from $K(\xi_{ik}) \equiv 0 \pmod{p}$; equivalently, from $G(\xi_{ik}) \not\equiv 0 \pmod{p}$ it follows that $K(\xi_{ik}) \not\equiv 0 \pmod{p}$. The normalization is needed only for this part of the induction. Under the substitution $\xi_{14} = \xi_{13}$, the individual products of powers of G do not vanish. A vanishing of K could therefore occur only because distinct products of powers in G correspond to equal products in K ; and that in turn can happen only when these products of powers differ merely by an interchange of the indices 3 and 4. Suppose that such a normalized product of powers is, for example,

$$\xi_{12}^{\tau_{12}} \xi_{13}^{\tau_{13}} \xi_{14}^{\tau_{14}} \xi_{24}^{\tau_{24}}.$$

Because of the assumed separate homogeneity in each index, a replacement of 3 by 4 in one ξ_{ik} must be accompanied by a replacement of 4 by 3 in another; a relevant term would therefore contain, instead of $\xi_{13}\xi_{24}$, the product $\xi_{14}\xi_{23}$, which is excluded by the normalization. In exactly the same way, against

$$\xi_{12}^{\tau_{12}} \xi_{13}^{\tau_{13}} \xi_{14}^{\tau_{14}} \xi_{24}^{\tau_{24}}$$

only a term containing the factor $\xi_{14}\xi_{23}$ could cancel, which is again excluded by the normalization. Hence $K(\xi_{ik}) \equiv 0 \pmod{p}$ implies $G(\xi_{ik}) \equiv 0 \pmod{p}$.

⁵⁸This sharper assertion means that each residue class contains only one normalized polynomial.

c) The case of n rows α_i, β_i

The case of n rows is now settled by complete induction, as an exact generalization of the just treated case of four rows.⁵⁹ First I again show that for every polynomial F there is a congruence

$$F(\xi_{ik}) \equiv F_0(\xi_{ik}) \pmod{\mathfrak{N}} \quad \text{identically in } \xi_{ik}, \quad (10)$$

where $\mathfrak{N} = (f_{ik,rs})$ and where $F_0(\xi_{ik})$ is normalized. The normalization is to consist in the following: if i, k, r, s are four different indices and $i < k < r < s$, then F_0 is not to contain the product $\xi_{is}\xi_{kr}$; that is, the indices of one ξ are not both to lie between those of the other. This normalization imposes no restriction in the case of two and three rows, where every polynomial is already normalized; in the case of four rows, as shown, there also exists a normalized polynomial for every residue class. The existence of a normalized polynomial for every residue class may therefore be assumed proved for $(n-1)$ rows.

Let an arbitrary product of powers in F be written in the form

$$\xi_{i_1 n} \cdots \xi_{i_\nu n} P,$$

where P no longer contains the index n . By the induction hypothesis, P is congruent modulo $\mathfrak{N}$ to an integral normalized polynomial P_0 :

$$\xi_{i_1 n} \cdots \xi_{i_\nu n} P \equiv \xi_{i_1 n} \cdots \xi_{i_\nu n} P_0 \pmod{\mathfrak{N}}.$$

If P_0 contains no ξ_{rs} such that for at least one index i_λ the two indices r, s lie between i_λ and n , i.e. $i_\lambda < r < s < n$, then the normalization has already been reached, since the hypotheses are fulfilled for the product of any two ξ 's from P_0 . Otherwise let i_λ be such an index, $i_\lambda < r < s < n$, and let P_0^* be the product of powers from P_0 containing ξ_{rs} . Since

$$\xi_{i_\lambda n} \xi_{rs} \equiv \xi_{i_\lambda s} \xi_{rn} - \xi_{i_\lambda r} \xi_{sn} \pmod{\mathfrak{N}},$$

one obtains

$$\begin{aligned} & \xi_{i_1 n} \cdots \xi_{i_\lambda n} \cdots \xi_{i_\nu n} P_0^* \\ & \equiv \xi_{i_1 n} \cdots \xi_{rn} \cdots \xi_{i_\nu n} Q + \xi_{i_1 n} \cdots \xi_{sn} \cdots \xi_{i_\nu n} R \pmod{\mathfrak{N}} \\ & \equiv \xi_{i_1 n} \cdots \xi_{rn} \cdots \xi_{i_\nu n} Q_0 + \xi_{i_1 n} \cdots \xi_{sn} \cdots \xi_{i_\nu n} R_0 \pmod{\mathfrak{N}}, \end{aligned}$$

where Q_0 and R_0 again denote the normalized polynomials of the residue classes of Q and R . These exist by the induction hypothesis, since Q and R do not contain the index n , and they are certainly integral polynomials, since Q and R are simply products of powers. Since $i_\lambda < r < s < n$, one also has

$$\begin{aligned} ((n - i_1) + \cdots + (n - r) + \cdots + (n - i_\nu)) &< ((n - i_1) + \cdots + (n - i_\lambda) + \cdots + (n - i_\nu)), \\ ((n - i_1) + \cdots + (n - s) + \cdots + (n - i_\nu)) &< ((n - i_1) + \cdots + (n - i_\lambda) + \cdots + (n - i_\nu)). \end{aligned}$$

Thus, in passing from P_0^* to Q_0, R_0 , this sum of differences has decreased; since the sum is necessarily $\geq \sigma$, the procedure must terminate after finitely many steps for each product of powers P_0^* . Hence

$$F(\xi_{ik}) = \sum \xi_{i_1 n} \cdots \xi_{i_\nu n} P^{(1)} \equiv \sum \xi_{j_1 n} \cdots \xi_{j_\sigma n} S_0^{(j)} = F_0(\xi_{ik}) \pmod{\mathfrak{N}},$$

where the integral polynomial $F_0(\xi_{ik})$ is necessarily normalized, since otherwise the difference sum could be lowered further. This proves (10). Since, by the induction hypothesis for $(n-1)$ indices, every separately homogeneous F has a separately homogeneous normalized F_0 , the procedure just given shows that this is also the case for n indices. Hence in what follows only separately homogeneous polynomials need be considered.

As in b), set

$$F_0(\xi_{ik}) = G(\xi_{ik}) + \xi_{n-1, n} F_1(\xi_{ik}),^{60} \quad (11)$$

⁵⁹The proof still applies for $n = 3$.

⁶⁰The identity corresponding to (10) and (11),

$$F((ik)) = F_0((ik)) = G((ik)) + (n-1, n) F_1((ik)),$$

is an analogue of the Clebsch-Gordan series expansion, as soon as the two rows $(n-1)$ and (n) are replaced by rows of variables x, y , so that $(n-1, n)$ is replaced by (xy) . But whereas Clebsch-Gordan involves an expansion by polars, the normalization of F_0 corresponds to "initial terms" of polars, and thereby forces the integrality which does not hold for Clebsch-Gordan. The known proof that, when integrality is disregarded, the $f_{ik,rs}$ form a basis of $\mathfrak{M}$ is carried out precisely by means of the Clebsch-Gordan series expansion (Gordan-Kerschensteiner, *Vorlesungen über Invariantentheorie*, p. 132).

where G contains no product of powers divisible by $\xi_{n-1,n}$, and put further

$$[G]_{\xi_{in}=\xi_{i,n-1}} = K(\xi_{ik}). \quad (12)$$

As the definition of normalization shows, K , as well as G , is normalized.

Again there is a one-to-one correspondence between G and K . Distinct products of powers from G can correspond to the same product in K only if they differ merely by an interchange of the indices n and $(n-1)$. Suppose, for instance, that G is of degree ρ in the index $(n-1)$ and of degree σ in the index n , and that

$$\chi_1 \leq \chi_2, \dots, \leq \chi_\rho \leq \chi_{\rho+1}, \dots, \leq \chi_{\rho+\sigma}$$

are the indices connected with $(n-1)$ and n in a product of powers of G . Their number must be $\rho + \sigma$, since by (11) the indeterminate $\xi_{n-1,n}$ does not occur in G . By the normalization, the product of powers is therefore of the form

$$\xi_{\chi_1, n-1} \cdots \xi_{\chi_\rho, n-1} \xi_{\chi_{\rho+1}, n} \cdots \xi_{\chi_{\rho+\sigma}, n} P(\xi_{ik}),$$

where $P(\xi_{ik})$ no longer contains the indices n and $(n-1)$. Each interchange of n with $(n-1)$ would, for $i \neq j$, give the factor $\xi_{in}\xi_{j,n-1}$ with $i < j$; hence $j, n-1$ lies between i and n , and the term would not be normalized. Thus, for fixed $\chi_1, \chi_2, \dots, \chi_{\rho+\sigma}$ and fixed P , G contains only one product of powers. This proves that different products of powers from G correspond to different products in K . Therefore

$$K(\xi_{ik}) \equiv 0 \pmod{p} \implies G(\xi_{ik}) \equiv 0 \pmod{p}. \quad (13)$$

From

$$F((ik)) \equiv 0 \pmod{p} \text{ identically in } \alpha, \beta$$

it follows now from (10), taking account of (2), that

$$F_0((ik)) \equiv 0 \pmod{p} \text{ identically in } \alpha, \beta. \quad (14)$$

Specializing $\alpha_n = \alpha_{n-1}$, $\beta_n = \beta_{n-1}$, (11) and (12) give

$$K((ik)) \equiv 0 \pmod{p} \text{ identically in } \alpha, \beta. \quad (15)$$

Since $K(\xi_{ik})$ is normalized and contains only $(n-1)$ indices, it follows by what was proved under a) and under b), formula (9), that

$$K(\xi_{ik}) \equiv 0 \pmod{p} \text{ identically in } \xi_{ik}.$$

Then by (13)

$$G(\xi_{ik}) \equiv 0 \pmod{p} \text{ identically in } \xi_{ik}.$$

Hence (11) gives

$$F_0(\xi_{ik}) \equiv \xi_{n-1,n} F_1(\xi_{ik}) \pmod{p} \text{ identically in } \xi_{ik}.$$

Since $(n, n-1) \not\equiv 0 \pmod{p}$ identically in α, β , it follows from (14) that

$$F_1((ik)) \equiv 0 \pmod{p} \text{ identically in } \alpha, \beta,$$

where $F_1(\xi_{ik})$ is again normalized and has lower degree in $\xi_{n-1,n}$ than F_0 . Repeating the process finitely many times yields

$$F_0(\xi_{ik}) \equiv \xi_{n-1,n}^\lambda F_\lambda(\xi_{ik}) \pmod{p},$$

where F_λ is of degree zero in $\xi_{n-1,n}$, and hence vanishes modulo p by what has just been proved. Thus one obtains

$$\begin{aligned} F_0(\xi_{ik}) &\equiv 0 \pmod{p} \text{ identically in } \xi_{ik}, \text{ or} \\ F(\xi_{ik}) &\equiv 0 \pmod{(\mathfrak{P}, p)} \text{ identically in } \xi_{ik}. \end{aligned} \quad (16)$$

This proves the converse of (2), and hence (1). At the same time, it proves in the case of n indices, and therefore in general, the sharper assertion used in the induction step for $F_0(\xi_{ik})$.

§ 4. Finiteness of the Integral Invariants of Finite Groups

The elementary proof of finiteness given in my note “The finiteness theorem for invariants of finite groups”⁶¹ admits, by means of the special finiteness theorems III and IV of § 1, the sharpening to integrality, whereas the usual proof based on Hilbert’s theorem on the module basis does not supply this integrality. Even the use of the integral module basis only gives a representation in which an arbitrarily high power of the integer h , the order of the group, appears in the denominator.

I use throughout the notation of the note just mentioned. Let the finite group $\mathfrak{H}$ consist of the h linear transformations $A_1, \dots, A_h$ of nonzero determinant,⁶² where A_k denotes the linear transformation

$$x_1^{(k)} = \sum_{\nu=1}^n a_{1\nu}^{(k)} x_\nu, \quad \dots, \quad x_n^{(k)} = \sum_{\nu=1}^n a_{n\nu}^{(k)} x_\nu,$$

or, briefly, $(x^{(k)}) = A_k(x)$. Thus the group $\mathfrak{H}$ sends the row (x) with elements $x_1, \dots, x_n$ into the rows $(x^{(k)})$ with elements $x_1^{(k)}, \dots, x_n^{(k)}$. The coefficients $a_{i\nu}^{(k)}$ are assumed to be algebraic integers; this is no restriction of generality, since by a theorem of J. Schur⁶³ every finite group of linear transformations is similar to one for which the $a_{i\nu}^{(k)}$ become algebraic integers.

By an integral absolute invariant of the group is meant a polynomial rational function of $x_1, \dots, x_n$, with algebraic integers of the number field $\mathfrak{K}$ generated by the $a_{i\nu}^{(k)}$ as coefficients, which remains identically unchanged under application of $A_1, \dots, A_h$. For such an invariant $f(x)$ one has

$$f(x) = f(x^{(1)}) = \dots = f(x^{(h)}) = \frac{1}{h} \sum_{k=1}^h f(x^{(k)}). \quad (1)$$

Conversely, every integral symmetric function of the h rows of quantities $(x^{(k)})$ also becomes an integral invariant of the group.

Let $\omega_1, \omega_2, \dots, \omega_\rho$ denote a basis of all integers of $\mathfrak{K}$. Then every invariant can be represented as

$$f(x) = \omega_1 f_1(x) + \dots + \omega_\rho f_\rho(x),$$

where $f_1(x), \dots, f_\rho(x)$ have rational integer coefficients. Thus by (1)

$$h f(x) = \omega_1 \sum_{k=1}^h f_1(x^{(k)}) + \dots + \omega_\rho \sum_{k=1}^h f_\rho(x^{(k)}).$$

Here the individual sums are symmetric functions of the h rows of quantities $(x^{(k)})$, and indeed with rational integer coefficients. By Theorem III they can therefore be expressed polynomially and rationally, with rational integer coefficients, in terms of finitely many integral-rational symmetric functions of these rows. By the preceding argument, these basis functions $I_1(x), \dots, I_\sigma(x)$ become integral invariants of the group, in general with algebraic-integral coefficients, since $\mathfrak{H}$ need not contain together with A all of its algebraically conjugate transformations.

There is therefore a representation

$$h \cdot f(x) = \omega_1 G_1(I) + \dots + \omega_\rho G_\rho(I), \quad (2)$$

where $G_1, \dots, G_\rho$ have rational integer coefficients.

Now let $w_1, \dots, w_\rho$ be indeterminates, and let

$$L = w_1 G_1(I) + \dots + w_\rho G_\rho(I)$$

run through all linear forms in the w ’s which, by the substitution $w_i = \omega_i/h$, correspond to invariants $f(x)$ in the representation (2). Hilbert’s theorem on the integral module basis gives

$$L = A_1(I) L_1 + \dots + A_\tau(I) L_\tau, \quad (3)$$

⁶¹*Math. Ann.* 77, p. 89 (1915).

⁶²It would suffice to suppose that $\mathfrak{H}$ is simply isomorphic to an abstract finite group; that is, if a transformation determinant of the A ’s vanishes, then $\mathfrak{H}$ should be similar to a group $\begin{pmatrix} \mathfrak{S} & 0 \\ 0 & 0 \end{pmatrix}$, where the determinants of the substitutions of $\mathfrak{S}$ do not vanish. In this case the invariants of $\mathfrak{H}$ coincide with the invariants of $\mathfrak{S}$, so the condition of the nonvanishing of the determinants is in fact no restriction of generality.

⁶³Über Gruppen linearer Substitutionen mit Koeffizienten aus einem algebraischen Zahlkörper. Satz VII. *Math. Ann.* 71, p. 555 (1912).

where the A_i have rational integer coefficients, and where, since all L 's are linear in the w 's, the A_i no longer contain the w 's. If the substitution $\omega_i = w_i/h$ sends $L_1, \dots, L_\tau$ to the invariants $\mathfrak{I}_1(x), \dots, \mathfrak{I}_\tau(x)$, then (3) becomes

$$f(x) = A_1(I)\mathfrak{I}_1(x) + \dots + A_\tau(I)\mathfrak{I}_\tau(x). \quad (4)$$

This representation shows that

$$I_1(x), \dots, I_\sigma(x); \mathfrak{I}_1(x), \dots, \mathfrak{I}_\tau(x)$$

form a basis of all integral invariants of the group $\mathfrak{H}$, such that every invariant is representable as a polynomial rational function, with rational integer coefficients, of these finitely many invariants.

If, in particular, the group $\mathfrak{H}$ has the property that with each transformation A it also contains all $A', A'', \dots$ with algebraically conjugate number coefficients, then the integral-rational symmetric functions of the h rows $(x^{(k)})$ become functions of x with rational integer coefficients. This holds in particular also for the basis functions of the symmetric functions. Thus, if one restricts oneself to invariants $f(x)$ with rational integer coefficients, then the basis functions

$$I_1(x), \dots, I_\sigma(x); \mathfrak{I}_1(x), \dots, \mathfrak{I}_\tau(x)$$

also have rational integer coefficients. Under this special assumption, which is in general not satisfied by the groups $\mathfrak{H}$, integral finiteness therefore also holds for the subdomain of invariants with rational integer coefficients.