

15. Die Endlichkeit des Systems der ganzzahligen Invarianten binärer Formen

Nachr. v. d. Ges. d. Wiss. zu Göttingen 1919, S. 138–156

Vorgelegt von F. Klein in der Sitzung vom 27. März 1919.

Im folgenden wird, als Erweiterung des bekannten Endlichkeitssatzes, der Satz bewiesen: Alle ganzen **ganzzahligen** Invarianten eines binären Grundformensystems sind ganze rationale, **ganzzahlige** Funktionen einer endlichen Anzahl unter ihnen. Dabei ist wie üblich, unter „Invariante“ immer eine ganze rationale Invariante einer Grundform oder eines Grundformensystems zu verstehen, und zwar eine Invariante gegenüber der durch die Gruppe aller linearen Transformationen induzierten Koeffiziententransformation.

Der Beweis beruht auf einer Ganzzahligkeits-Verschärfung des Mertens-Hilbertschen Endlichkeitsbeweises¹⁾. Dieser Endlichkeitsbeweis läßt sich so charakterisieren: Man zerlegt die Grundformen in ihre Linearfaktoren — präziser ausgedrückt: man ordnet jeder Grundform ein Produkt von Linearformen zu —, wodurch jede Invariante I in eine Invariante dieser Linearformen, also in eine Funktion der homogen gemachten Wurzeln übergeht. Diese Funktion hat drei Bedingungen zu genügen: 1) Der Bedingung der Invarianz, 2) Gewichtsbedingungen, 3) Symmetriebedingungen. Die Bedingungen 2) und 3) sind notwendig, damit I ganz und rational in den Koeffizienten der Grundformen wird. Der Bedin-

1) F. Mertens, Wiener Sitzungsberichte Jan. 1889; D. Hilbert, Math. Ann. Bd. 33 (1889) [datiert März 1888]. Die beiden, unabhängig von einander im Anschluß an Mertens, Crelle Bd. 100 entstandenen Beweise stimmen inhaltlich überein.

gung 1) wird dadurch genügt, daß I als ganze rationale Funktion der Determinanten der Linearformen dargestellt wird; der Bedingung 2) dadurch, daß statt der einzelnen Determinanten gewisse ihrer Potenzprodukte als neue Argumente genommen werden. Die Bedingung 3) sagt jetzt einfach aus, daß I eine ganze rationale, symmetrische Funktion von Größenreihen wird, und daß umgekehrt jede solche symmetrische Funktion von Größenreihen eine Invariante der Grundformen wird. Die symmetrischen Elementarfunktionen dieser Größenreihen ergeben also das vollständige System.

Betrachtet man nun nur ganzzahlige Invarianten, so läßt sich der Bedingung 1) ebenso wie oben genügen, sobald für Invarianten von Linearformen der schärfere Satz bewiesen ist, daß alle **ganzzahligen** Invarianten binärer Linearformen ganze **ganzzahlige** Funktionen der Determinanten dieser Linearformen sind. Daß dies tatsächlich zutrifft, zeige ich in § 3, und zwar in der Fassung, daß die Gesamtheit aller modulo irgend einer Primzahl zwischen diesen Determinanten bestehenden Relationen übereinstimmt mit der Gesamtheit aller identischen Relationen; daß also der diesen Relationen entsprechende Modul ein Primmodul modulo jeder Primzahl bleibt. Dieser Nachweis geschieht durch Normierung der Restklassen inbezug auf den Modul der quadratischen Formen, die den quadratischen Relationen zwischen den Determinanten entsprechen; diese quadratischen Formen ergeben sich dabei als ganzzahlige Basis des Moduls, und zwar modulo jeder Primzahl; während sie bisher nur unter Vernachlässigung der Ganzzahligkeit als Modulbasis bekannt waren.

Um der Bedingung 2) zu genügen, ist keine Abänderung nötig, da die Einführung der Potenzprodukte die Zahlkoeffizienten nicht beeinflußt. Die Bedingung 3) sagt jetzt aus, daß $n_1! \dots n_\mu! I$ (wo $n_1, \dots, n_\mu$ die Gradzahlen der einzelnen Grundformen bedeuten) eine ganzzahlige symmetrische Funktion von Größenreihen wird, und daß umgekehrt jede ganzzahlige symmetrische Funktion dieser Reihen eine ganzzahlige Invariante wird. Nun besitzen aber, wie sich leicht zeigen läßt, diese ganzzahligen symmetrischen Funktionen von Reihen eine ganzzahlige Basis, zu der allerdings die Elementarfunktionen nicht mehr ausreichen. Die Anwendung des Hilbertschen Theorems von der ganzzahligen Modulbasis ergibt daraus auch für die I selbst eine ganzzahlige Basis.

§ 1 stellt die den Bedingungen 1), 2), 3) entsprechenden speziellen Endlichkeitssätze zusammen, woraus dann in § 2 der End-

lichkeitsbeweis folgt. Die der Bedingung 3) entsprechenden speziellen Endlichkeitssätze ergeben zugleich die Endlichkeit der ganzzahligen Invarianten endlicher Gruppen ganzzahliger oder algebraisch-ganzzahliger Substitutionen, wie in § 4 noch kurz ausgeführt wird.

§ 1. Spezielle Endlichkeitssätze.

Ich schiebe die folgenden speziellen Endlichkeitssätze voraus, die dazu dienen werden, den in der Einleitung erwähnten Bedingungen der Invarianz, des Gewichts und der Symmetrie zu genügen:

I. Jede ganzzahlige Invariante eines Systems binärer Linearformen ist eine ganze rationale, ganzzahlige Funktion der Determinanten dieser Linearformen (der Beweis wird in § 3 erbracht werden).

II. Jedes System $\mathfrak{S}$ von Potenzprodukten von n Variabeln mit nichtnegativen Exponenten, das neben irgend zwei Potenzprodukten f und g auch deren Quotienten enthält, sobald dieser Quotient **ganz** in den Variabeln ist, besitzt eine endliche multiplikative Basis $f_1, \dots, f_k$ von Funktionen aus $\mathfrak{S}$, derart daß für jedes f aus $\mathfrak{S}$ eine Darstellung gilt: $f = f_1^{\lambda_1} \dots f_k^{\lambda_k}$, mit nicht-negativen Exponenten $\lambda_1, \dots, \lambda_k$.

Nach dem Hilbertschen Satz von der Modulbasis existiert nämlich eine endliche Anzahl von Funktionen aus $\mathfrak{S}$: $f_1, \dots, f_k$, die sämtlich die x wirklich enthalten, derart daß jedes nicht-konstante f aus $\mathfrak{S}$ dem daraus abgeleiteten Modul angehört: $f \equiv 0 \pmod{(f_1 \dots f_k)}$. Daraus folgt, daß zu jedem $f = x_1^{i_1} \dots x_n^{i_n}$ mindestens ein $f_v = x_1^{v_1} \dots x_n^{v_n}$ existiert derart daß $v_1 \leq i_1; \dots, v_n \leq i_n$. In der Darstellung:

$$f = x_1^{i_1 - v_1} \dots x_n^{i_n - v_n} f_v = A f_v^1)$$

1) Diese Darstellung läßt sich auch direkt beweisen, und daraus folgt dann umgekehrt wieder der Hilbertsche Satz: vergl. P. Gordan: Neuer Beweis des Hilbertschen Satzes über homogene Funktionen, Gött. Nachr. 1899. Ein anderer direkter Beweis dieser Darstellung, aus der dann auch Satz II abgeleitet wird, bei A. Ostrowski: Über die Existenz einer endlichen Basis bei gewissen Funktionensystemen (Math. Ann. 78, 1916) § 2, 1 und § 3, 2.

Der in § 2 benutzte Spezialfall von Satz II, wo die Exponenten alle nicht-negativen Lösungen eines Diophantischen Gleichungssystems durchlaufen, findet sich schon bei Gordan-Kerschensteiner: Vorlesungen über Invariantentheorie, Bd. I, S. 199.

gehört nach Voraussetzung A zu $\mathfrak{S}$, hat aber niedrigeren Grad in den Variablen als f , so daß durch endlich oftmalige Wiederholung der Schlußweise die Behauptung folgt (damit die Darstellung auch noch für $f = 1$ gilt, sind nur alle Exponenten λ gleich Null zu setzen).

III. Alle ganzen ganzzahligen symmetrischen Funktionen von n Größenreihen sind ganze, ganzzahlige Funktionen einer endlichen Anzahl unter ihnen.

Denn bezeichnen $\tau_1(x), \dots, \tau_n(x)$ die elementaren symmetrischen Funktionen der Unbestimmten $x_1 \dots x_n$, so gilt für jeden Exponenten k eine Identität:

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

wo $G_0^{(k)}, \dots, G_{n-1}^{(k)}$ ganze, ganzzahlige Funktionen der $\tau(x)$ bedeuten. Es seien nun $x_i, y_i \dots z_i$ die Elemente der i ten Reihe; dann werden vermöge dieser Identitäten und entsprechender für die $y \dots z$ alle speziellen (einförmigen) symmetrischen Funktionen:

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

ganze ganzzahlige Funktionen der endlich vielen:

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

und der elementaren symmetrischen Funktionen $\tau(x), \tau(y) \dots \tau(z)$ ¹⁾.

Hat man den im folgenden nicht auftretenden Fall der allgemeinsten symmetrischen Funktionen der n Reihen, so zeigt sich ebenso, daß die Funktionen

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

wo $i_1, i_2 \dots i_n$ alle Permutationen durchläuft, zusammen mit den $\tau(x), \tau(y) \dots \tau(z)$ eine ganzzahlige Basis bilden.

IV. Es seien $F_1(x), \dots, F_k(x)$ ganze ganzzahlige Funktionen von $x_1 \dots x_n$; a eine feste ganze Zahl. Dann sind alle Funktionen $\frac{G(F)}{a}$, wo G eine ganze ganzzahlige Funktion bedeutet, die ganzzahlig in den

1) Hilbert nimmt a. a. O. anstelle der $\tau(x), \dots, \tau(z)$ die Potenzsummen in die Basis auf, wodurch auch diese nur aus einförmigen Funktionen besteht, aber die Ganzzahligkeit der Darstellung verloren geht.

x werden, ganze ganzzahlige Funktionen einer endlichen Anzahl unter ihnen.

Denn nach dem Hilbertschen Satz von der ganzzahligen Modulbasis gilt für jedes solche $\frac{G(F)}{a}$ eine Darstellung:

$$\frac{G(F)}{a} = A_1(F_1 \dots F_k) \frac{G_1(F)}{a} + \dots + A_q(F_1 \dots F_k) \frac{G_q(F)}{a},$$

wo $A_1, \dots, A_q$ ganze ganzzahlige Funktionen der F bedeuten, und $\frac{G_1(F)}{a}, \dots, \frac{G_q(F)}{a}$ zum System gehören. Die Funktionen

$$F_1 = \frac{a F_1}{a}; \dots F_k = \frac{a F_k}{a}; \quad \frac{G_1(F)}{a}, \dots \frac{G_q(F)}{a}$$

bilden also die gewünschte Basis.

§ 2. Endlichkeit der ganzzahligen binären Invarianten.

Es seien x, y binäre Veränderliche, die einer Transformation mit unbestimmten Koeffizienten

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

unterworfen werden; f eine binäre Grundform, deren Koeffizienten Unbestimmte seien. Dann gilt vermöge (1):

$$(2) \quad f = a_0 x^n + a_1 x^{n-1} y + \dots + a_n y^n = a'_0 x'^n + a'_1 x'^{n-1} y' + \dots + a'_n y'^n.$$

Unter einer ganzzahligen Invariante von f versteht man bekanntlich eine ganze ganzzahlige Funktion $I(a)$, derart daß

$$(3) \quad I(a') = |s_{ik}|^q I(a), \quad (\text{identisch in } a, s_{ik})^1);$$

entsprechend sind die ganzzahligen Invarianten eines Grundformensystems zu definieren, wobei noch die Homogenität in den Koeffizienten der einzelnen Grundformen mit in die Definition aufgenommen werden kann, da aus solchen einzeln-homogenen Invarianten sich die übrigen ganzzahlig-linear zusammensetzen lassen.

Ich betrachte nun neben (2) noch eine spezielle binäre Form g , nämlich das Produkt von n Linearformen, deren Koeffizienten wieder Unbestimmte seien:

1) Schreibt man, wie vielfach in der Invariantentheorie üblich, f mit Binomialkoeffizienten: $f = b_0 x^n + \binom{n}{1} b_1 x^{n-1} y + \dots + b_n y^n$, so wird der Bereich aller ganzzahligen Invarianten $I(b)$ gegenüber dem der $I(a)$ erweitert, und die angewandten Endlichkeitsschlüsse versagen; $I(b)$ wird keine ganzzahlige Funktion der Wurzeln mehr.

$$\begin{aligned}
 (4) \quad g &= (\alpha_1 x + \beta_1 y)(\alpha_2 x + \beta_2 y) \dots (\alpha_n x + \beta_n y) \\
 &= \sigma_0(\alpha, \beta) x^n + \sigma_1(\alpha, \beta) x^{n-1} y + \dots \sigma_n(\alpha, \beta) y^n \\
 &= (\alpha'_1 x' + \beta'_1 y')(\alpha'_2 x' + \beta'_2 y') \dots (\alpha'_n x' + \beta'_n y') \\
 &= \sigma'_0 x'^n + \sigma'_1 x'^{n-1} y' + \dots \sigma'_n y'^n,
 \end{aligned}$$

wo also $\sigma_0(\alpha, \beta), \sigma_1(\alpha, \beta) \dots \sigma_n(\alpha, \beta)$ die homogen gemachten symmetrischen Elementarfunktionen bedeuten, und die transformierten Koeffizienten σ'_i gleich $\sigma_i(\alpha', \beta')$ werden.

Wegen der algebraischen Unabhängigkeit dieser Elementarfunktionen entspricht jeder Relation:

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

eine weitere:

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

und somit für Unbestimmte $a_0, \dots a_n$:

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

Nun entspricht jeder ganzzahligen Invariante $I(a)$ von f durch die Substitution $a_i = \sigma_i(\alpha, \beta)$ eine ganzzahlige Invariante $I(\sigma) = H(\alpha, \beta)$ von g , wo H eine ganzzahlige Funktion von α, β wird, für diese Invariante geht die Relation (3) über in:

$$(8) \quad I(\sigma') = |s_{ik}|^q I(\sigma) \quad [\text{identisch in } \sigma, s_{ik}],$$

und wegen $\sigma' = \sigma(\alpha', \beta')$ folgt aus (8):

$$(9) \quad H(\alpha', \beta') = |s_{ik}|^q H(\alpha, \beta) \quad [\text{identisch in } \alpha, \beta; s_{ik}];$$

$I(\sigma) = H(\alpha, \beta)$ wird also eine ganzzahlige Invariante der n Linearformen $(\alpha_i x + \beta_i y)$. Es sei nun umgekehrt $H(\alpha, \beta)$ eine ganzzahlige Invariante dieser n Linearformen, also (9) erfüllt, und es sei zugleich $H(\alpha, \beta)$ gleich einer ganzzahligen Funktion $I(\sigma)$ der σ . Da dann auch

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

wird, schreibt sich (9) auch:

$$(9a) \quad I(\sigma') = |s_{ik}|^q I(\sigma) \quad [\text{identisch in } \alpha, \beta; s_{ik}];$$

und daraus folgt nach (5) und (6) auch (8); und nach (7) auch (3). Es entspricht somit jeder ganzzahligen Invariante $I(a)$ eine ganzzahlige Invariante $H(\alpha, \beta) = I(\sigma)$ der n Linearformen, und umgekehrt. Bedeutet ferner $I_1(a), \dots I_k(a)$ eine ganzzahlige Basis aller $I(a)$, so wird $H_1(\alpha, \beta), \dots H_k(\alpha, \beta)$ eine ganzzahlige Basis aller $H(\alpha, \beta)$, die zugleich ganzzahlige

Funktionen $I(\sigma)$ sind; und auch hier gilt nach (5), (6), (7) die Umkehrung. Um also die Existenz einer ganzzahligen Basis für alle $I(a)$ nachzuweisen, genügt der Nachweis für alle ganzzahligen Invarianten $H(\alpha, \beta)$, die zugleich ganzzahlige Funktionen $I(\sigma)$ sind; und die Basis $H_1(\alpha, \beta) = I_1(\sigma), \dots, H_k(\alpha, \beta) = I_k(\sigma)$ liefert für die $I(a)$ die Basis $I_1(a), \dots, I_k(a)$.

Es durchlaufe nun $H(\alpha, \beta) = I(\sigma)$ die Gesamtheit aller ganzzahligen Invarianten von (4). Da wegen (3) jede Invariante homogen in den σ wird, und nach (4) jedes σ homogen und linear in den Koeffizienten jeder Linearform ist, wird also $H(\alpha, \beta)$ homogen in jeder Reihe $\alpha_i \beta_i$ und in jeder Reihe von gleicher Dimension; außerdem natürlich eine symmetrische Funktion der n Reihen. Umgekehrt wird jede ganzzahlige symmetrische Funktion $H(\alpha, \beta)$ der n Reihen, die einzeln homogen und gleicher Dimension in jeder Reihe ist, nach dem Fundamentalsatz über die symmetrischen Funktionen eine ganze, ganzzahlige Funktion der σ ; also nach dem obigen eine Invariante $I(\sigma)$, sobald $H(\alpha, \beta)$ invariant ist. Die Gesamtheit der ganzzahligen Invarianten von (4) ist also charakterisiert als Gesamtheit der ganzzahligen Funktionen $H(\alpha, \beta)$ mit folgenden Eigenschaften:

- 1) Ganzzahlige Invariante der n Linearformen $\alpha_i x + \beta_i y$;
- 2) Einzeln homogen und gleicher Dimension in jeder der n Reihen α_i, β_i ;
- 3) Symmetrisch in den n Reihen α_i, β_i .

Nach dem speziellen Endlichkeits-Satz I wird $H(\alpha, \beta)$ wegen 1) eine ganze, ganzzahlige Funktion der Determinanten

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

also

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

In dieser Darstellung läßt sich die Symmetrie auch formal zum Ausdruck bringen, indem man auf $G((ik))$ alle Permutationen der n Reihen anwendet:

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

G^* enthält also neben jedem Potenzprodukt P der (ik) auch die Summe $Q = P^{(1)} + \dots + P^{(n!)}$ über alle Permutationen von P ; und zwar wird G^* eine ganzzahlige, lineare Kombination endlich vieler Q , $G^* = \sum c Q$. Da die Q den Bedingungen 1), 2), 3) genügen, also selbst Invarianten werden, genügt es die Q anstelle von $G^*((ik))$ zu betrachten.

Es durchlaufe nun P das System $\mathfrak{S}$ aller in den Q auftretenden, d. h. der Bedingung 2) genügenden Potenzprodukte der (ik) . Ist der Quotient zweier P ganz in den (ik) , so genügt er ebenfalls der Bedingung 2), gehört also zu $\mathfrak{S}$. Nach Satz II gibt es somit eine endliche Anzahl derartiger P , etwa $P_1, \dots, P_q$ derart, daß jedes P sich darstellen läßt in der Form

$$P = P_1^{\lambda_1} \dots P_q^{\lambda_q}$$

mit nicht-negativen Exponenten λ . Durch Anwendung aller Permutationen erhält man daraus:

$$Q = P_1^{(1)\lambda_1} \dots P_q^{(1)\lambda_q} + \dots + P_1^{(n!)\lambda_1} \dots P_q^{(n!)\lambda_q};$$

Q wird also eine ganzzahlige symmetrische Funktion der $n!$ Größenreihen von je q Elementen:

$$P_1^{(1)} \dots P_q^{(1)}; P_1^{(2)} \dots P_q^{(2)}; \dots; P_1^{(n!)} \dots P_q^{(n!)};$$

also nach Satz III eine ganze ganzzahlige Funktion endlich vieler symmetrischer Funktionen dieser Reihen. Diese Basisfunktionen werden selbst Größen Q oder symmetrische Elementarfunktionen der $n!$ Elemente $P_i^{(1)}, P_i^{(2)} \dots P_i^{(n!)}$, genügen somit den Bedingungen 1) 2) 3) und werden ganzzahlige Invarianten

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

Nach (10) wird somit wegen $G^* = \sum c Q$ jedes $H(\alpha, \beta) = I(\sigma)$ von der Form:

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

wo Φ eine ganze ganzzahlige Funktion bedeutet; und umgekehrt wird $\frac{1}{n!} \Phi$ eine ganzzahlige Invariante, sobald es ganz in α, β wird. Es lassen sich also nach Satz IV den Invarianten (11) noch endlich viele $I_{l+1}(\sigma), \dots, I_k(\sigma)$ zufügen, derart daß

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

eine ganzzahlige Basis aller Invarianten $H(\alpha, \beta) = I(\sigma)$ bilden, womit der Satz für den Fall einer Grundform bewiesen ist.

Handelt es sich um ein Grundformensystem, so kann, wie oben bemerkt, Homogenität der Invarianten in den Koeffizienten jeder Grundform vorausgesetzt werden. Man ersetzt nun wieder die allgemeinen Grundformen durch solche, die jeweils das Produkt

von Linearformen sind. Deren Invarianten werden dann: 1) Invarianten dieser Linearformen; 2) einzeln homogen in den aus den Koeffizienten der Linearformen gebildeten Reihen, und gleicher Dimension in den Reihen jeder einzelnen Grundform; 3) symmetrisch in den Reihen jeder einzelnen Grundform. Umgekehrt entspricht wieder jeder ganzzahligen Invariante aller Linearformen, die diesen Bedingungen genügt, eine ganzzahlige Invariante des Grundformensystems. Der Beweis verläuft dem angegebenen absolut parallel; auf jedes, den Gewichtsbedingungen genügende Potenzprodukt $P = P_1^{j_1} \dots P_\rho^{j_\rho}$ der einzelnen Determinanten (Satz I und II) sind alle $N = n_1! \dots n_\rho! \dots n_\mu!$ Permutationen anzuwenden, wo $n_1, \dots, n_\mu$ die Gradzahlen der Grundformen bedeuten. Dadurch geht $N.I$ über in eine ganzzahlige symmetrische Funktion von N Reihen aus je ρ Elementen, woraus die ganzzahlige Basis für alle $N.I$ und folglich nach Satz IV die ganzzahlige Basis für alle I sich ergibt.

§ 3. Die Basis der ganzzahligen Invarianten binärer Linearformen.

Es ist jetzt noch der Beweis des speziellen Endlichkeitssatzes I nachzutragen. Nach einem bekannten, zuerst von Clebsch bewiesenen Satz sind alle ganzen rationalen Invarianten der n Linearformen $\alpha_i x + \beta_i y$ ganze rationale Funktionen der Determinanten (ik) . Insbesondere werden also alle ganzzahligen Invarianten dieser Linearformen ganze rationale, aber nicht notwendig ganzzahlige Funktionen dieser Determinanten.

Im folgenden wird gezeigt, daß vermöge der zwischen den (ik) bestehenden identischen Relationen diese Darstellung auch stets ganzzahlig möglich ist.

In Formeln und in der Sprache der Modultheorie drückt sich das so aus: Es seien ξ_{ik} , wo $i < k$, Unbestimmte; dann bildet die Gesamtheit aller ganzzahligen Polynome $F(\xi_{ik})$ von der Eigenschaft, daß $F((ik))$ identisch in α, β verschwindet, einen Modul $\mathfrak{M}$; da die Summe zweier F und ebenso das Produkt eines F mit einem beliebigen ganzzahligen Polynom der ξ_{ik} auch dieser Gesamtheit angehört. In Formeln: aus

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

folgt

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

und umgekehrt.

Ich zeige nun, daß ganz entsprechend gilt: Aus

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

(1) folgt

$$F(\xi_{ik}) \equiv 0 \pmod{\mathfrak{M}, p} \quad [\text{identisch in } \xi_{ik}],$$

und umgekehrt, und zwar für jede Primzahl p . Dadurch ist $\mathfrak{M}$ also auch identisch mit dem der Gesamtheit aller Relationen der (ik) modulo p entsprechenden Modul $\mathfrak{M}_p$, der aus allen ganzzahligen Polynomen $F(\xi_{ik})$ besteht, für die $F((ik))$ modulo p identisch in α, β verschwindet.

Daß (1) die ganzzahlige Darstellbarkeit aussagt, zeigt sich so: (1) läßt sich auch in der Form schreiben:

$$\text{Aus } F((ik)) = p \cdot H(\alpha, \beta) \quad [\text{identisch in } \alpha, \beta] \text{ folgt:}$$

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

also nach der Definition von $\mathfrak{M}$:

$$F((ik)) = p \cdot G((ik)) \quad [\text{identisch in } \alpha, \beta]^1).$$

Somit ergibt sich: $p \cdot H(\alpha, \beta) = p \cdot G((ik))$ oder: $H(\alpha, \beta) = G((ik))$.

Liegt also eine Darstellung vor:

$$H(\alpha, \beta) = \frac{1}{p_1^{\lambda_1} \dots p_q^{\lambda_q}} F((ik)),$$

wo $p_1, \dots, p_q$ Primzahlen bedeuten, so folgt daraus auch:

$$H(\alpha, \beta) = \frac{1}{p_1^{\lambda_1-1} \dots p_q^{\lambda_q}} G((ik)),$$

woraus durch endlich oftmalige Wiederholung sich die Ganzzahligkeit der Darstellung ergibt.

Zum Nachweis von (1) bezeichne

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

die den quadratischen Relationen zwischen den (ik) :

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

entsprechenden Formen der Unbestimmten ξ_{ik} ; $\mathfrak{N} = (f_{ik,rs})$ den aus ihnen abgeleiteten Modul aus ganzzahligen Polynomen. Aus

$$F(\xi_{ik}) \equiv 0 \pmod{\mathfrak{N}} \quad \text{folgt also: } F((ik)) = 0 \quad [\text{identisch in } \alpha, \beta],$$

(2) Aus

$$F(\xi_{ik}) \equiv 0 \pmod{(\mathfrak{N}, p)} \quad , \quad , \quad F((ik)) \equiv 0 \pmod{p} \quad [\text{identisch in } \alpha, \beta].$$

1) Dieser letztere Schluß beweist zugleich die Umkehrung von (1).

Ich zeige nun, vermöge einer Normierung der Restklassen inbezug auf $\mathfrak{N}$, daß auch die Umkehrung von (2) gilt, womit $\mathfrak{N} = \mathfrak{M} = \mathfrak{M}_p$ und damit (1) bewiesen sein wird. Dabei ergibt sich $\mathfrak{N} = \mathfrak{M}$ als Spezialfall von $\mathfrak{N} = \mathfrak{M}_p$ für $p = 0$; der Fall $p = 0$ ist in den folgenden Überlegungen stets mit enthalten. Anders ausgedrückt: Die $f_{ik,rs}$ bilden eine ganzzahlige Modulbasis von $\mathfrak{M}_p$, insbesondere auch von $\mathfrak{M}_0 = \mathfrak{M}$.

a) Fall von zwei oder drei Reihen $\alpha_i \beta_r$. Da noch keine vier verschiedenen Indices auftreten, wird $\mathfrak{N}$ der Nullmodul. Es ist also zu zeigen, daß aus

$$(3) \quad \begin{aligned} F((ik)) &\equiv 0 \bmod p \text{ [identisch in } \alpha, \beta] \text{ folgt:} \\ F(\xi_{ik}) &\equiv 0 \bmod p \text{ [identisch in } \xi_{ik}], \end{aligned}$$

womit (1) mit $\mathfrak{M} = \mathfrak{M}_p = 0$ bewiesen sein wird.

Da die Bedingung $F(ik) = p \cdot H(\alpha, \beta)$ für die in den einzelnen Reihen homogenen Bestandteile einzeln erfüllt sein muß, genügt es durchweg, $F((ik))$ in jeder einzelnen Reihe homogen, also $F(\xi_{ik})$ in jedem Index homogen, anzunehmen. Nun gibt es im Fall von zwei Reihen nur die eine Determinante (12) und die entsprechende Unbestimmte ξ_{12} . Wegen der angenommenen Homogenität wird also: $F = c \cdot \xi_{12}^*$. Aus

$$c \cdot (12)^* \equiv 0 \bmod p \text{ [identisch in } \alpha, \beta]$$

folgt aber wegen $(12) \not\equiv 0 \bmod p$ [identisch in α, β] stets $c \equiv 0 \bmod p$: also

$$F(\xi_{ik}) \equiv 0 \bmod p \text{ [identisch in } \xi_{ik}],$$

womit (3) und somit (1) bewiesen ist.

Im Fall von drei Reihen gibt es die Determinanten (12), (13), (23), denen die Unbestimmten ξ_{12} , ξ_{13} , ξ_{23} entsprechen; es wird also

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

Sei nun F bezw. von den Gradzahlen $\sigma_1, \sigma_2, \sigma_3$ in den Indices 1, 2, 3; dann gilt also das Gleichungssystem

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

mit der eindeutigen Umkehrung:

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

sodaß jedes einzeln homogene F höchstens einen Term enthält;

$F = c \cdot \xi_{12}^{\tau_{12}} \xi_{13}^{\tau_{13}} \xi_{23}^{\tau_{23}}$, woraus wie oben das Erfülltsein von (3) und folglich (1) sich ergibt.

b) Fall von 4 Reihen α_i, β_i . Es treten die sechs Unbestimmten $\xi_{12}, \xi_{13}, \xi_{14}, \xi_{23}, \xi_{24}, \xi_{34}$ und die entsprechenden Determinanten auf; und es wird $\mathfrak{N} = (f_{12, 34})$. Wegen

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

ist jedes Potenzprodukt der ξ_{ik} modulo $\mathfrak{N}$ einer linearen ganzzahligen Kombination solcher Potenzprodukte kongruent, in denen das Produkt $\xi_{14} \xi_{23}$ nicht auftritt. Für jedes Polynom $F(\xi_{ik})$ gilt also:

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

wo F_0 das Produkt $\xi_{14} \xi_{23}$ nicht enthält; F_0 soll als das normierte Polynom der Restklasse von F bezeichnet werden. Dabei entspricht einem einzeln homogenen F , da (4) einzeln homogen ist, wieder ein einzeln homogenes F_0 .

Ich setze nun:

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

wo G kein durch ξ_{34} teilbares Potenzprodukt enthält, und weiter:

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

Aus

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

folgt nun nach (5) unter Berücksichtigung von (2):

$$(8) \quad F_0((ik)) \equiv 0 \pmod{p} \text{ [identisch in } \alpha, \beta];$$

und daraus durch die Spezialisierung $\alpha_4 = \alpha_3, \beta_4 = \beta_3$ nach (6) und (7):

$$K(ik) \equiv 0 \pmod{p} \text{ [identisch in } \alpha, \beta].$$

Also gilt nach dem unter a) Bewiesenen:

$$K(\xi_{ik}) \equiv 0 \pmod{p} \text{ [identisch in } \xi_{ik}],$$

und hieraus folgt, was noch unten zu zeigen ist:

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

Es wird also nach (6): $F_0(\xi_{ik}) \equiv \xi_{34} \cdot F_1(\xi_{ik}) \pmod{p}$ [identisch in ξ_{ik}]; und wegen (34) $\not\equiv 0 \pmod{p}$ [identisch in α, β] folgt aus (8) auch:

$$F_1((ik)) \equiv 0 \pmod{p} \text{ [identisch in } \alpha, \beta];$$

wo $F_1(\xi_{ik})$ wieder normiert und von niedrigerem Grad in ξ_{34} ist. Die endlich oftmalige Wiederholung des Verfahrens führt somit zu:

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

wo F_λ nullten Grades in ξ_{34} ist, also nach dem eben Bewiesenen modulo p verschwindet. Somit ergibt sich:

$$(9) \quad \begin{aligned} F_0^*(\xi_{ik}) &\equiv 0 \pmod{p} \text{ [identisch in } \xi_{ik}], \text{ oder} \\ F(\xi_{ik}) &\equiv 0 \pmod{(\mathfrak{N}, p)} \text{ [identisch in } \xi_{ik}], \end{aligned}$$

womit die Umkehrung von (2) und damit (1) bewiesen ist; zugleich in der schärferen Aussage für $F_0(\xi_{ik})^1$.

Es ist noch nachzutragen, daß aus $K(\xi_{ik}) \equiv 0 \pmod{p}$ auch $G(\xi_{ik}) \equiv 0 \pmod{p}$ folgt; d. h. aus $G(\xi_{ik}) \not\equiv 0 \pmod{p}$ auch $K(\xi_{ik}) \not\equiv 0 \pmod{p}$; nur zu diesem Teil des Induktionsschlusses wird die Normierung gebraucht. Da durch die Substitution $\xi_{14} = \xi_{13}$ die einzelnen Potenzprodukte von G nicht verschwinden, könnte ein Verschwinden von K nur dadurch eintreten, daß verschiedenen Potenzprodukten in G gleiche in K entsprechen; und das kann wieder nur dann der Fall sein, wenn diese Potenzprodukte sich nur um eine Vertauschung der Indices 3 und 4 unterscheiden. Sei nun ein solches, nach Voraussetzung normiertes, Potenzprodukt etwa gegeben durch $\xi_{12}^{\tau_{12}} \xi_{13}^{\tau_{13}} \xi_{14}^{\tau_{14}} \xi_{24}^{\tau_{24}}$. Wegen der vorausgesetzten Einzelhomogenität in jedem Index muß einem Ersetzen von 3 durch 4 in einem ξ_{ik} ein Ersetzen von 4 durch 3 in einem andern entsprechen; ein inbetrachtkommendes Glied würde also statt $\xi_{13} \xi_{24}$ das Produkt $\xi_{14} \xi_{23}$ enthalten, was durch die Normierung ausgeschlossen ist. Ganz entsprechend könnte gegen $\xi_{12}^{\tau_{12}} \xi_{13}^{\tau_{13}} \xi_{14}^{\tau_{14}} \xi_{24}^{\tau_{24}}$ wieder nur ein Glied sich aufheben, das den Faktor $\xi_{14} \xi_{23}$ enthält, was durch die Normierung ausgeschlossen ist. Somit folgt aus $K(\xi_{ik}) \equiv 0 \pmod{p}$ auch $G(\xi_{ik}) \equiv 0 \pmod{p}$.

c) Der Fall von n Reihen α_i, β_i läßt sich nun durch volle Induktion erledigen, in genauer Verallgemeinerung des eben behandelten Falles von vier Reihen²⁾. Ich zeige zuerst wieder, daß für jedes Polynom F eine Kongruenz statthat:

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

wo also $\mathfrak{N} = (f_{ik}, r_s)$ und wo $F_0(\xi_{ik})$ normiert ist. Die Normierung soll dabei in folgendem bestehen: Sind i, k, r, s vier verschiedene Indices, und $i < k < r < s$, so soll F_0 das Produkt $\xi_{is} \xi_{kr}$ nicht enthalten; d. h. es sollen die Indices des einen ξ nicht beide zwischen denen des andern liegen. Diese Normierung stellt noch keine Einschränkung dar für den Fall von zwei und drei Reihen, wo also jedes Polynom normiert

1) Diese schärfere Aussage bedeutet, daß jede Restklasse nur ein einziges normiertes Polynom enthält.

2) Der Beweis gilt auch noch für $n = 3$.

ist; auch im Fall von vier Reihen existiert, wie gezeigt, ein normiertes Polynom für jede Restklasse. Die Existenz eines normierten Polynoms für jede Restklasse kann also für $(n-1)$ Reihen als bewiesen angenommen werden.

Ein beliebiges Potenzprodukt von F sei in der Form geschrieben:

$$\xi_{i_1 n} \dots \xi_{i_\sigma n} P,$$

wo P den Index n nicht mehr enthält. Nach Voraussetzung ist also P einem ganzzahligen normierten Polynom $P_0 \bmod \mathfrak{N}$ kongruent:

$$\xi_{i_1 n} \dots \xi_{i_\sigma n} P \equiv \xi_{i_1 n} \dots \xi_{i_\sigma n} P_0 \bmod \mathfrak{N}.$$

Enthält nun P_0 kein ξ_{rs} derart, daß für mindestens einen Index i dies r, s zwischen i_λ und n liegt ($i_\lambda < r < s < n$), so ist die Normierung schon erreicht, da für das Produkt irgend zweier ξ aus P_0 die Voraussetzungen erfüllt sind. Andernfalls sei i_λ ein solcher Index, daß $i_\lambda < r < s < n$; und P_0^* das ξ_{rs} enthaltende Potenzprodukt aus P_0 ; wegen

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

kommt dann:

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

wo Q_0 und R_0 wieder die normierten Polynome der Restklassen von Q und R bedeuten; Q_0 und R_0 existieren nach Voraussetzung, da Q und R den Index n nicht enthalten, und sind sicher ganzzahlige Polynome, da Q und R einfach Potenzprodukte sind. Wegen $i_\lambda < r < s < n$ folgt aber auch:

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

Durch den Übergang von P_0^* zu Q_0, R_0 hat also diese Differenzensumme abgenommen; und da diese Summe notwendig $\geq \sigma$ ist, muß das Verfahren für jedes Potenzprodukt P_0^* nach endlich vielen Schritten abbrechen. Somit kommt:

$$F(\xi_{ik}) = \sum \xi_{i_1 n} \dots \xi_{i_\sigma n} \cdot P^{(\sigma)} \equiv \sum \xi_{j_1 n} \dots \xi_{j_\sigma n} \cdot S_0^{(\sigma)} = F_0(\xi_{ik}) \bmod \mathfrak{N},$$

wo das ganzzahlige Polynom $F_0(\xi_{ik})$ notwendig normiert ist, da sich sonst die Differenzensumme noch weiter erniedrigen ließe; damit ist (10) bewiesen. Da weiter nach Voraussetzung bei $(n-1)$

Indices jedem einzeln homogenen F ein einzeln homogenes normiertes F_0 entspricht, zeigt das angegebene Verfahren, daß dies auch für n Indices der Fall ist; es handelt sich daher im folgenden nur um einzeln homogene Polynome.

Ich setze nun wieder, analog wie unter b):

$$(11) \quad F_0(\xi_{ik}) = G(\xi_{ik}) + \xi_{n-1, n} F_1(\xi_{ik})^4,$$

wo G kein durch $\xi_{n-1, n}$ teilbares Potenzprodukt enthält, und weiter:

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

wie die Definition der Normierung zeigt, ist neben G auch K normiert.

Dann besteht wieder zwischen G und K ein-eindeutiges Entsprechen; denn es können nur solchen verschiedenen Potenzprodukten aus G gleiche in K entsprechen, die sich nur um eine Vertauschung der Indices n und $(n-1)$ unterscheiden. Sei nun etwa G vom Grade ϱ im Index $(n-1)$, vom Grade σ im Index n , und seien $\kappa_1 \leq \kappa_2 \leq \dots \leq \kappa_\varrho \leq \kappa_{\varrho+1} \leq \dots \leq \kappa_{\varrho+\sigma}$ die in einem Potenzprodukt von G mit $(n-1)$ und n verbundenen Indices, deren Anzahl $\varrho + \sigma$ sein muß, da nach (11) die Unbestimmte $\xi_{n-1, n}$ in G nicht auftritt. Dann ist wegen der Normierung das Potenzprodukt von der Form:

$$\xi_{\kappa_1, n-1} \dots \xi_{\kappa_\varrho, n-1} \xi_{\kappa_{\varrho+1}, n} \dots \xi_{\kappa_{\varrho+\sigma}, n} \cdot P(\xi_{ik}),$$

wo $P(\xi_{ik})$ die Indices n und $(n-1)$ nicht mehr enthält. Jede Vertauschung von n mit $(n-1)$ gibt für $i \neq j$ den Faktor: $\xi_{in} \xi_{j, n-1}$ mit $i < j$; so daß also $j, n-1$ zwischen i und n liegt, das Glied nicht normiert wäre. G enthält somit zu festen $\kappa_1, \kappa_\varrho, \dots, \kappa_{\varrho+\sigma}$ und festem P nur ein Potenzprodukt, womit gezeigt ist, daß verschiedenen Potenzprodukten aus G verschiedene in K entsprechen.

$$(13) \quad \text{Aus } K(\xi_{ik}) \equiv 0 \pmod{p} \text{ folgt somit } G(\xi_{ik}) \equiv 0 \pmod{p}.$$

1) Die (10) und (11) entsprechende Identität:

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

stellt ein Analogon zu der Clebsch-Gordanschen Reihenentwicklung dar, sobald man die beiden Reihen $(n-1)$ und (n) durch Variablenreihen x, y , also $(n-1, n)$ durch (xy) ersetzt. Während es sich aber bei Clebsch-Gordan um Entwicklung nach Polaren handelt, entspricht die Normierung von F_0 „Anfangsgliedern“ von Polaren, und dadurch läßt sich die bei Clebsch-Gordan nicht geltende Ganzzahligkeit erzwingen. Der bekannte Beweis, daß unter Vernachlässigung der Ganzzahligkeit die $f_{ik, rs}$ eine Basis von $\mathfrak{M}$ bilden, wird gerade vermöge der Clebsch-Gordanschen Reihenentwicklung geführt (Gordan-Kerschensteiner: Vorlesungen über Invariantentheorie S. 132).

Aus

$$F((ik)) \equiv 0 \bmod p \text{ [identisch in } \alpha, \beta]$$

folgt nun nach (10) unter Berücksichtigung von (2):

$$(14) \quad F_0((ik)) \equiv 0 \bmod p \text{ [identisch in } \alpha, \beta]$$

und daraus durch die Spezialisierung: $\alpha_n = \alpha_{n-1}$, $\beta_n = \beta_{n-1}$ nach (11) und (12):

$$(15) \quad K((ik)) \equiv 0 \bmod p \text{ [identisch in } \alpha, \beta].$$

Da $K(\xi_{ik})$ normiert ist und nur $(n-1)$ Indices enthält, kann nach dem unter a) und unter b) (9) Bewiesenen wegen (15) vorausgesetzt werden:

$$K(\xi_{ik}) \equiv 0 \bmod p \text{ [identisch in } \xi_{ik}]$$

und daraus folgt nach (13):

$$G(\xi_{ik}) \equiv 0 \bmod p \text{ [identisch in } \xi_{ik}].$$

Nach (11) kommt also:

$$F_0(\xi_{ik}) \equiv \xi_{n-1, n} F_1(\xi_{ik}) \bmod p \text{ [identisch in } \xi_{ik}],$$

und wegen $(n, n-1) \not\equiv 0 \bmod p$ [identisch in α, β] folgt aus (14) auch:

$$F_1((ik)) \equiv 0 \bmod p \text{ [identisch in } \alpha, \beta];$$

wo $F_1(\xi_{ik})$ wieder normiert und von niedrigerem Grad in $\xi_{n-1, n}$ als F_0 ist. Die endlich oftmalige Wiederholung des Verfahrens führt somit zu:

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

wo F_λ nullten Grades in $\xi_{n-1, n}$ ist, also nach dem eben Bewiesenen modulo p verschwindet. Somit ergibt sich:

$$(16) \quad \begin{aligned} F_0(\xi_{ik}) &\equiv 0 \bmod p \text{ [identisch in } \xi_{ik}] \text{ oder} \\ F(\xi_{ik}) &\equiv 0 \bmod (\mathfrak{N}, p) \text{ [identisch in } \xi_{ik}] \end{aligned}$$

Damit ist aber die Umkehrung von (2) und folglich (1) bewiesen; und zugleich für $F_0(\xi_{ik})$ die beim Induktionsschluß benutzte schärfere Aussage auch im Falle von n Indices, also allgemein-giltig, bewiesen.

§ 4. Die Endlichkeit der ganzzahligen Invarianten endlicher Gruppen.

Der in meiner Note „der Endlichkeitssatz der Invarianten endlicher Gruppen“¹⁾ gegebene elementare Endlichkeitsbeweis läßt vermöge der speziellen Endlichkeitssätze III und IV des § 1 die Verschärfung auf Ganzzahligkeit zu; während der gewöhnliche, auf den Hilbertschen Satz von der Modulbasis sich stützende Beweis diese Ganzzahligkeit nicht liefert. Denn auch die Heranziehung der ganzzahligen Modulbasis gibt nur eine Darstellung, bei der eine beliebig hohe Potenz der ganzen Zahl h — der Ordnung der Gruppe — in den Nenner tritt.

Ich schließe mich durchweg den Bezeichnungen der erwähnten Note an. Die endliche Gruppe $\mathfrak{G}$ bestehe aus den h linearen Transformationen (von nicht verschwindender Determinante)²⁾ $A_1 \dots A_h$, wobei durch A_k die lineare Transformation:

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

oder abkürzend $(x^{(k)}) = A_k(x)$ dargestellt sei. Die Gruppe $\mathfrak{G}$ führt also die Reihe (x) mit den Elementen $x_1, \dots, x_n$ über in die Reihen $(x^{(k)})$ mit den Elementen $x_1^{(k)}, \dots, x_n^{(k)}$. Dabei seien die Koeffizienten $a_{i\nu}^{(k)}$ als ganze algebraische Zahlen vorausgesetzt; das bedeutet insofern keine Beschränkung der Allgemeinheit, als nach einem Satz von J. Schur³⁾ jede endliche Gruppe linearer Transformationen einer solchen ähnlich ist, für die die $a_{i\nu}^{(k)}$ ganze algebraische Zahlen werden.

Unter einer ganzzahligen (absoluten) Invariante der Gruppe sei eine solche ganze rationale Funktion von $x_1, \dots, x_n$ verstanden, mit ganzen Zahlen des aus den $a_{i\nu}^{(k)}$ abgeleiteten algebraischen Zahlkörpers $\mathfrak{K}$ als Koeffizienten,

1) Math. Ann. 77, S. 89 (1915).

2) Es würde genügen, vorauszusetzen, daß $\mathfrak{G}$ einer abstrakten endlichen Gruppe einstufig isomorph ist; d. h. wenn eine Transformationsdeterminante der A verschwindet, soll $\mathfrak{G}$ einer Gruppe $\begin{pmatrix} \mathfrak{G} & 0 \\ 0 & 0 \end{pmatrix}$ ähnlich sein, wo die Determinanten der Substitutionen von $\mathfrak{G}$ nicht verschwinden. Die Invarianten von $\mathfrak{G}$ decken sich aber in diesem Fall mit den Invarianten von $\mathfrak{G}$, sodaß die Bedingung des Nichtverschwindens der Determinanten tatsächlich keine Beschränkung der Allgemeinheit vorstellt.

3) Über Gruppen linearer Substitutionen mit Koeffizienten aus einem algebraischen Zahlkörper. Satz VII. Math. Ann. 71. S. 355 (1912).

die bei Anwendung von $A_1 \dots A_h$ identisch ungeändert bleibt; für eine solche Invariante $f(x)$ gilt also:

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

Umgekehrt wird auch jede ganzzahlige symmetrische Funktion der h Größenreihen $(x^{(k)})$ eine ganzzahlige Invariante der Gruppe.

Es bezeichne nun $\omega_1, \omega_2 \dots \omega_q$ eine Basis aller ganzen Zahlen aus $\mathfrak{R}$, so daß jede Invariante sich darstellen läßt als

$$f(x) = \omega_1 f_1(x) + \dots + \omega_q f_q(x),$$

wo $f_1(x), \dots, f_q(x)$ ganze rationale Zahlkoeffizienten besitzen. Nach (1) kommt somit:

$$h \cdot f(x) = \omega_1 \sum_{k=1}^h f_1(x^{(k)}) + \dots + \omega_q \sum_{k=1}^h f_q(x^{(k)}).$$

Hier sind die einzelnen Summen symmetrische Funktionen der h Größenreihen $(x^{(k)})$, und zwar mit ganzen rationalen Zahlkoeffizienten; also nach Satz III ganz und rational, mit ganzen rationalen Zahlkoeffizienten, durch endlich viele ganzrationalzahlige symmetrische Funktionen dieser Reihen ausdrückbar. Diese Basisfunktionen $I_1(x), \dots, I_\sigma(x)$ werden dabei nach dem obigen ganzzahlige Invarianten der Gruppe, mit im allgemeinen ganzen algebraischen Zahlkoeffizienten, da $\mathfrak{H}$ neben A nicht alle algebraisch-konjugierten Transformationen enthalten wird.

Es gilt somit eine Darstellung

$$(2) \quad h \cdot f(x) = \omega_1 G_1(I) + \dots + \omega_q G_q(I),$$

wo $G_1, \dots, G_q$ ganze rationale Zahlkoeffizienten besitzen.

Sind nun $w_1, \dots, w_q$ Unbestimmte, und durchläuft

$$L = w_1 G_1(I) + \dots + w_q G_q(I)$$

alle Linearformen der w , denen durch die Substitution $w_i = \frac{\omega_i}{h}$

Invarianten $f(x)$ in der Darstellung (2) entsprechen, so ergibt sich nach dem Hilbertschen Satz von der ganzzahligen Modulbasis

$$(3) \quad L = A_1(I) L_1 + \dots + A_r(I) L_r,$$

wo die A_i ganze rationale Zahlkoeffizienten besitzen und wo wegen der Linearität aller L in den w die A_i die w nicht mehr enthalten.

Entsprechen nun durch die Substitution: $\omega_i = \frac{w_i}{h}$ den $L_1 \dots L_r$

die Invarianten $\mathfrak{I}_1(x) \dots \mathfrak{I}_r(x)$, so geht (3) durch diese Substitution über in:

$$(4) \quad f(x) = A_1(I) \cdot \mathfrak{I}_1(x) + \dots + A_r(I) \mathfrak{I}_r(x).$$

Diese Darstellung (4) zeigt, daß $I_1(x), \dots, I_o(x); \mathfrak{I}_1(x), \dots, \mathfrak{I}_r(x)$ eine Basis aller ganzzahligen Invarianten der Gruppe $\mathfrak{H}$ bilden, derart, daß jede Invariante sich ganz und rational, mit ganzen rationalen Zahlkoeffizienten, durch diese endlich vielen darstellen läßt.

Hat die Gruppe $\mathfrak{H}$ insbesondere die Eigenschaft, daß sie neben jeder Transformation A auch alle $A', A'' \dots$ mit algebraisch-konjugierten Zahlkoeffizienten enthält, so werden die ganzrationalen symmetrischen Funktionen der h Reihen $(x^{(k)})$ Funktionen von x mit ganzen rationalen Zahlkoeffizienten; dies gilt insbesondere auch von den Basisfunktionen der symmetrischen Funktionen. Beschränkt man sich also auf Invarianten $f(x)$ mit ganzen rationalen Zahlkoeffizienten, so besitzen auch die Basisfunktionen $I_1(x), \dots, I_o(x); \mathfrak{I}_1(x) \dots \mathfrak{I}_r(x)$ ganze rationale Zahlkoeffizienten. Es gilt also unter dieser speziellen, im allgemeinen für die Gruppen $\mathfrak{H}$ nicht erfüllten Voraussetzung, die ganzzahlige Endlichkeit auch für den Teilbereich der ganzrationalen Invarianten.