Hilbert, D.

Über die Theorie der algebraischen Formen. (German) JFM 22.0133.01

Math. Ann. 36, 473-534 (1890).

Der Verfasser ist zu den Ergebnissen der vorliegenden Untersuchung, welche vier früher erschienene Noten [Gött. Nachr. 1888, 450–457 (1888; JFM 20.0109.01), Gött. Nachr. 1889, 25–34, 423–430 (1889; JFM 21.0102.01)] zu einen einheitlichen Ganzen verarbeitet, durch die Aufgabe geführt worden, die bisher nur für Systeme von binären und für die einfachsten ternären Formen nachgewiesene Existenz "voller Systeme von Grundformen", durch welche sich alle weiteren invarianten Bildungen der Unformen ganz-rational ausdrücken lassen, auf Systeme beliebiger Formen mit beliebigen Variabelnreihen auszudehnen.

Indem er aber dieses sein erstes Ziel dadurch erreicht, dass er den Kern der Frage von dem engeren Gebiet der Invariantentheorie loslöst und als eine fundamentale Eigenschaft von unendlichen Systemen algebraischer Formen überhaupt statuirt, gelingt es ihm, darüber hinaus eine Reihe von Sätzen nachzuweisen, welche die von Kronecker einerseits, von Dedekind und Weber andererseits begründete Theorie der algebraischen Moduln weiterführen und zugleich bemerkenswerte Anwendungen auf Zahlentheorie, Algebra und Geometrie zulassen.

Wir versuchen, zunächst den erstgenannten Gegenstand im Zussammenhange darzulegen.

Man denke sich ein Gesetz gegeben, nach welchem eine unendliche Reihe von Formen $F_1, F_2, \dots$ der n Variabeln $x_1, x_2, \dots, x_n$ fortschreitet. Dabei sollen die Ordnungen der F keiner Beschränkung unterliegen, während von deren Coefficienten nur angenommen wird, dass sie irgend einem "Rationalitätsbereiche" R angehören. Dann lautet der Hauptsatz (A):

"Aus der Reihe der F lässt sich stets eine endliche Anzahl derselben $F_{i_1}, F_{i_2}, \dots, F_{i_m}$ derart herausgreifen, dass jede Form F_s der Reihe in der Gestalt darstellbar ist:

$$F_s = A_{s_i}F_{i+1} + A_{s_2}F_{i_2} + \cdots + A_{s_m}F_{i_m},$$

wo die A ebenfalls Formen der x sind, mit Coefficienten des nämlichen Rationalitätsbereiches R."

Es sei nämlich F irgend ein Individuum der Reiche, von der Ordnung R in den x. Es darf angenommen werden, dass der Coefficient von x_n^r in F nicht verschwindet. Zieht man nun die mit einer geeigneten Hülfsform B multiplicirte Form F von der Form F_s ab, lässt sich dadurch stets der Grad in x_n von F_s unter r herabdrücken, und es kommt:

$$F_s = B_sF + g_{s_1}x_n^{r-1} + g_{s_2}x_n^{r-2} + \cdots + g_{s_r},$$

wo die g nur noch von den $x_1, x_2, \dots, x_{n-1}$ abhängen, während ihre Ordnung in denselben eventuell beliebig hoch steigt.

Man nehme jetzt den Satz für Formen von $n-1$ Variabeln als richtig an und wende ihn auf die Coefficientencolonne der g_{s_1} an. Dann muss es möglich sein, aus den obigen Darstellungen der F_s eine endliche Anzahl μ (etwa für $s = 1, 2, \dots, \mu$) so herauszugreifen, dass nach beiderseitiger Multiplication mit geeigneten Hülfsformen der $x_1, x_2, \dots, x_{n-1}$, Addition und schliesslicher Subtraction von der Darstellung für jede Form F_s die letztere sich linear zusammensetzt aus $F, F_1, F_2, \dots, F_\mu$ und einer Form, deren Grad in x_n höchstens der $(r-2)^{\text{te}}$ ist.

Das nämliche Verfahren wird angewandt auf die Colonne der nunmehr mit der höchsten Potenz von x_n multiplicirten Coefficienten der neuen Darstellungen für $F_{\mu+1}, F_{\mu+2}, \dots$, so gelangt man nach höchstens r Schritten der Art zu einer endlichen Anzahl von Formen F, aus denen sich in der angegebenen Weise alle übrigen linear componiren.

Da der einfachste Fall $n = 1$ fast unmittelbar evident ist, so ist der Satz (A) damit bewiesen. Während bei der Durchführung des mitgeteilten Verfahrens das Auftreten rationaler Verbindungen der ursprünglichen Coefficienten unvermeidlich ist, lässt sich bei umgekehrter Reihenfolge der einzelnen Schritte erreichen, dass nur ganze und ganzzahlige Verbindungen der gegebenen Coefficienten eingeführt werden, womit eine Verwertung für Zwecke der Zahlentheorie möglich wird.

Es liege nun etwa eine einzelne ternäre Urform f vor, so kann man das System der (ganz-rationalen) Invarianten $i_1, i_2, \dots$ von f in eine einfach unendliche Reihe anordnen; für die der Satz (A) gilt. Man hat also für jede Invariante i eine Darstellung der Art:

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

die indessen noch so umgeformt werden muss, dass die A nur von den $i_1, i_2, \dots, i_m$ abhängen. Dies gelingt mit Hülfe einer Eigenschaft des Ω-Processes:

$$\Omega = \frac{\partial^3}{\partial a_{11} \partial a_{22} \partial a_{33}} - \frac{\partial^3}{\partial a_{11} \partial a_{23} \partial a_{32}} \pm \cdots - \frac{\partial^3}{\partial a_{13} \partial a_{22} \partial a_{31}},$$

wo die a_{ik} die Coefficienten einer linearen Transformation bedeuten, durch welche f in f' übergehe. Hat man nämlich eine isobare Form der Coefficienten von f', die man noch mit einer (positiven) Potenz der Transformations-Determinante multipliciren mag, und übt auf dieses Product den Process Ω so oft aus, bis die a_{ik} ganz herausgehen, so resultirt eine Invariante von f.

Die vorstehenden Betrachtungen gelten analog für ein System von Urformen mit Reihen von n Variabeln, die sogar auch ganz oder teilweise verschiedenen Substitutionen unterliegen können.

Selbst für gewisse Untergruppen der allgemeinen linearen Substitutionsgruppe bleibt der Beweis in Kraft.

Andererseits kann man mit denselben Mitteln auch die Existenz voller Systeme von "Syzyganten" nachweisen.

Zunächst hat man im Satze (A) nur eine der n Variabeln der Einheit gleich zu setzen, um den Satz auch für nicht homogene ganze Functionen brauchbar zu machen.

Nun herrschen zwischen den Invarianten einer Reihe von Urformen unbegrenzt viele Relationen ("Syzygien"), welche in den ursprünglichen Coefficienten identisch erfüllt sind. Die Syzyganten, d. h. die linken Seiten der Relationen, sind aber nicht homogene Formen, als deren Variabeln die Grundformen des vollen Systems anzusehen sind, so dass man, wie oben, vorgehen kann u. s. f.

Die Syzyganten sind abermals durch eine unbegrenzte Anzahl von identisch in jenen Grundformen erfüllten Relationen verknüpft. Die linken Seiten, die "Syzyganten zweiter Art", besitzen daher wiederum ein volles System etc.

Es erhebt sich jetzt von neuem die Frage, ob dieser Process der fortgesetzten Syzygienbildung nach einer endlichen Zahl von Malen abbricht oder nicht. Durch ein nicht ganz einfaches Schlussverfahren beweist der Verf. die Richtigkeit der ersteren Annahme.

Um eine vollständige Einsicht in die Structur der aus einer vorgelegten Reihe von Urformen entspringenden invarianten Formen zu gewinnen, muss man volle Systeme nicht nur für jene Invarianten, sondern auch für deren successive Syzyganten aufstellen.

Wir erwähnen nunmehr noch einige Anwendungen des Satzes (A) auf die oben berührten "Modulsysteme". Ein Modul ist insbesondere ein System von unbegrenzt vielen Formen derart, dass jedes Product einer Systemform mit einer ganz beliebigen anderen Form, und zugleich jede Summe solcher Producte, wiederum dem Systeme angehört.

Der Satz (A) gilt demnach auf für Moduln. Beispielsweise bilden die linken Seiten der Gleichungen der Flächen, welche durch eine algebraische Raumcurve gehen, einen Modul. Die Anwendung des Satzes (A) löst damit ein bekanntes Problem aus der Geometrie der Raumcurven. Um auch ein rein algebraisches Beispiel zu geben, so bilden einen Modul diejenigen Formen der Coefficienten einer gegebenen Gleichung, welche verschwinden, wenn die Gleichung eine gewisse Anzahl vielfacher Wurzeln besitzt.

Das wichtigste Ergebnis ist wohl die Schaffung eines neuen, fundamentalen Begriffes, der "charakteristischen Function χ" eines Moduls. Sei das "volle System" des Moduls bezeichnet mit $(F_1, F_2, \dots, F_m)$, so heisst gemäss Kronecker eine Form nach dem Modul der Null congruent, wenn sie aus den m Formen F_i linear ableitbar ist.

Die Zahl der von einander unabhängigen Bedingungen, welchen die Coefficienten einer Form F der R^{ten} Ordnung genügen müssen, damit dieselbe nach dem Modul $(F_1, F_2, \dots, F_m)$ der Null congruent sei, erweist sich für genügend grosse Werte von R gleich einer ganzen rationalen "charakteristischen Function $\chi(R)$" mit rationalen Zahlencoefficienten.

Zugleich wird eine Methode zur wirklichen Bildung einer solchen Function $\chi(R)$ angegeben.

Zwischen den charakteristischen Functionen zweier Moduln herrscht die einfache Beziehung, dass ihre Summe gleich ist der Summe der charakteristischen Functionen für den "kleinsten enthaltenden" und den "grössten gemeinsamen" Modul. Die beiden letzteren Moduln werden gebildet durch die gemeinsamen Formen der beiden gegebenen Moduln, resp. durch Zusammensetzung der beiden gegebenen Moduln. Dies findet seine Anwendung auf die Anzahl der gemeisamen Schnittpunkte zweier Raumcurven von den Geschlechtern p_1, p_2, welche zusammen den vollständigen Durchschnitt zweier Flächen von den Ordnungen r_1, r_2 bilden. Die gesuchte Anzahl ist dann $-2r_1r_2 + \frac{1}{2}r_1r_2(r_1 + r_2) - (p_1 + p_2) + 2$.

Reviewer: Meyer, F., Prof. (Clausthal)

MSC:

11E81	Algebraic theory of quadratic forms; Witt groups and rings	Cited in **22** Reviews Cited in **156** Documents

Full Text: DOI EuDML