Zur Theorie der Moduln und Ideale.

Von

E. Lasker in New-York.

Kapitel I.

Eliminationssätze.

1. Es sollen im folgenden einige Sätze über Systeme von Formen bewiesen werden, deren Resultante nicht verschwindet. Neben den Sätzen I, II, III, welche neu und für vielerlei Anwendungen der vorliegenden Untersuchung von Bedeutung sind, sind einige Sätze, vornämlich Satz IV und V, aufgestellt, die bereits bekannt und Gegenstand strengster Forschung gewesen sind. Dies könnte befremden und bedarf daher der Erläuterung. In zwei späteren Kapiteln (nämlich III und IV) werden die Grundlagen der Untersuchung, wie sie bis dorthin vorgeschritten ist, erweitert werden, und zwar in der Weise, daß ganze Serien von Schlüssen aus den vorangehenden Kapiteln übernommen werden können. Es ist daher zweckmäßig, die Beweise der bekannten Sätze von vornherein so zu stellen, daß ihre Übertragbarkeit auf die modifizierenden Verhältnisse ohne weiteres einleuchtet. Dies geschieht, indem jene Beweise auf das geringste Maß von Voraussetzungen gegründet werden.

Die Voraussetzungen, von denen die folgende Untersuchung ausgeht, mögen daher genau präzisiert werden. Sie sollen sich beschränken auf

1) die formalen Grundgesetze der Algebra und Arithmetik,
2) den Irreduzibilitätsbegriff der Formen,
3) den Zerlegungssatz der Formen in irreduzible Teiler,
4) den Gaußschen Fundamentalsatz über binäre Formen im komplexen Zahlgebiete,
5) die Eigenschaften der Determinanten,
6) die Eigenschaften der Resultante zweier binärer Formen,
7) die Theorie der symmetrischen Funktionen der Wurzeln einer Gleichung beliebigen Grades.

Dazu sollen noch einige funktionentheoretische Begriffe und Sätze treten, die sich auf Konvergenzbetrachtungen und Grenzübergänge einfacher Art zurückführen lassen.

Obwohl die Mittel der Untersuchung auf diese Weise sehr beschränkte sein sollen, so wird doch die Notation und Symbolik der neueren Mathematik, z. B. der Invariantentheorie, benutzt werden. Es ist dies keine Inkonsequenz, da diese Notationen und Symbole keinerlei Sätze anderer Art als die angeführten voraussetzen, ja in ihrer Mehrheit auf rein arithmetische Folgerungen aus den Rechnungsgesetzen der Algebra sich stützen.

2. Zunächst geben wir in knappen Worten den Ideengang des Nachweises der folgenden Tatsachen: Sind $x_1, \cdots, x_m$ m Variable, $f_1, \cdots, f_h, \cdots$ homogene Formen derselben, wird ein bestimmtes Wertsystem der Proportionen $x_1 : x_2 : \cdots : x_m$ „Punkt" genannt, so haben, wenn die Koeffizienten der $f_1, \cdots, f_m$ unbestimmt sind, die Gleichungen

$$f_1 = 0, \quad \cdots, \quad f_m = 0$$

keinen Punkt gemein. Dagegen haben $m-1$ solcher Gleichungen immer zum mindesten *einen* Punkt gemein. $f_1 = 0, \cdots, f_m = 0$ haben nur dann und immer dann einen Punkt gemein, wenn die Koeffizienten eine bestimmte Relation erfüllen. Dieselbe ist durch das Verschwinden einer Invariante von $f_1, \cdots, f_m$, der Resultante, ausdrückbar. Wird die Resultante von $f_1, \cdots, f_m$, deren Koeffizienten Unbestimmte sind, mit R bezeichnet und ist l eine Linearform mit unbestimmten Koeffizienten, so kann man immer eine positive ganze Zahl M und ganzzahlige Formen $p_1, \cdots, p_m$ nicht bloß der $x_1, \cdots, x_m$, sondern auch der unbestimmten Koeffizienten von $f_1, \cdots, f_m$ und l finden, so daß identisch

$$R \cdot l^M = p_1 \cdot f_1 + \cdots + p_m f_m$$

ist.

Wir erweisen die Behauptung durch Induktion, von $m-1$ Variablen auf m Variable schließend. Jene Sätze sind nach dem oben Gesagten bereits als erwiesen angenommen für $m = 2$. Machen wir nun die Annahme, daß sie für $m-1$ Variable richtig seien, und betrachten wir irgend eine der m Variablen, z. B. x_m, als unbestimmte Linearform der übrigen Variablen, sie etwa $= \eta x_1$ setzend. Alsdann sind

$$f_1, \cdots, f_{m-1}$$

$m-1$ Formen der $m-1$ Variablen $x_1, \cdots, x_{m-1}$, deren Koeffizienten Polynome von η mit unbestimmten Koeffizienten sind. Die notwendige und hinreichende Bedingung für eine gemeinsame Wurzel der Gleichungen $f_i = 0$ ist das Verschwinden der Resultante, die ein Polynom von η sein wird, das von η nicht unabhängig sein kann, da ja in dem speziellen Falle, wo die f_i Linearformen oder Produkte von Linearformen sind, diese

Resultantenform nicht von η unabhängig ist. Somit haben $f_1, \cdots, f_{m-1}$ in der Tat eine endliche Anzahl von Nullwerten gemein.

Bezeichnen wir die den gemeinsamen Punkten $P_1, P_2, \cdots, P_\alpha$ entsprechenden Linearformen ebenfalls mit $P_1, \cdots, P_\alpha$ und schreiben wir die Linearinvariante zweier kontragredienter Formen F, Φ derselben Ordnung symbolisch $F \times \Phi$, und bezeichnen wir mit μ die Ordnung von f_m, so ist $f_m \times P_1^\mu \cdot f_m \times P_2^\mu \cdots f_m \times P_\alpha^\mu$ dann und nur dann gleich Null, wenn $f_1, \cdots, f_m$ einen gemeinsamen Punkt besitzen. Dieser Wert

$$f_m \times P_1^\mu \cdot f_m \times P_2^\mu \cdots f_m \times P_\alpha^\mu$$

ist eine Form der Unbestimmten von $f_1, \cdots, f_m$, wie jetzt zu zeigen ist.

$\Theta = P_1 \cdot P_2 \cdots P_\alpha$ ist eine Form der Unbestimmten von $f_1, \cdots, f_{m-1}$ und der kontragredienten Variabelen $\xi_1, \cdots, \xi_m$ von $x_1, \cdots, x_m$. Wir können nämlich statt des Systems von Variablen

$$x_1, \cdots, x_{m-1}, x_m$$

das andere $x_1, \cdots, x_{m-1}, y = \xi_1 x_1 + \cdots + \xi_m x_m$ einführen und $f_1, \cdots, f_{m-1}$ nach Potenzen dieser Variablen geordnet denken, wobei, weil ja

$$\xi_m x_m = y - \xi_1 x_1 - \cdots - \xi_{m-1} x_{m-1},$$

nur eine Potenz von ξ_m als Nenner auftritt. Die Resultante R von $f_1, \cdots, f_{m-1}$ als Formen von $x_1, \cdots, x_{m-1}$, wenn y noch $= \eta x_1$ gesetzt wird, ist nach der Annahme des Induktionsschlusses eine Form der Koeffizienten von $f_1, \cdots, f_{m-1}$, als Formen von $x_1, \cdots, x_m$ betrachtet, von den $\xi_1, \cdots, \xi_m$ und von η. R ist mit einem Nenner behaftet, der eine Potenz von ξ_m ist, und den wir einfach fortlassen. $R = 0$, als Gleichung für η betrachtet, definiert dann die Werte von η, für welche $f_1 = 0, \cdots, f_{m-1} = 0$. R ist nach dem Gaußschen Fundamentalsatz als Produkt darstellbar, wo jeder der Faktoren linear von η abhängt:

$$R = A(\eta - a_1)(\eta - a_2) \cdots (\eta - a_\alpha),$$

nur einer derselben, A, von η nicht abhängt.

Ist nun $P_1 \equiv a_{1,1} : a_{1,2} : \cdots : a_{1,m}$ ein den $f_1, \cdots, f_{m-1}$ gemeinsamer Nullpunkt, so muß einer der Linearfaktoren von R, z. B. $\eta - a_1$, durch das Einsetzen jener Werte von $x_1, \cdots, x_m$ verschwinden.

ηx_1 war $= y = \xi_1 x_1 + \cdots + \xi_m x_m$, somit ist

$$\eta x_1 - a_1 x_1 = 0,$$

wenn

$$x_1 = a_{1,1}, \cdots, x_m = a_{1,m}.$$

Auch ist a_1 nur von den $\xi_1, \cdots, \xi_m$ und den Koeffizienten von $f_1, \cdots, f_{m-1}$ abhängig. Also ist

$$\xi_1 a_{1,1} + \xi_2 a_{1,2} + \cdots + \xi_m a_{1,m} = a_1 \cdot a_{1,1}$$

d. h.

$$P_1 = a_1 \cdot a_{1,1}.$$

Ebenso ist

$$P_\alpha = a_\alpha \cdot a_{\alpha,1}.$$

Aus $R = A(\eta - a_1) \cdots (\eta - a_\alpha)$ folgt für $\eta = 0$

$$(R)_{\eta=0} = A a_1 \cdot a_2 \cdots a_\alpha.$$

A wie $(R)_{\eta=0}$ sind Formen der Unbestimmten von $f_1, \cdots, f_{m-1}$ und der $\xi_1, \cdots, \xi_m$. Es zeigt sich also, daß

$$P_1 \cdot P_2 \cdots P_\alpha = (\xi_1 a_{1,1} + \cdots + \xi_m a_{1,m})(\xi_1 a_{2,1} + \cdots + \xi_m a_{2,m}) \cdots = \Theta$$

eine berechenbare Form der Unbestimmten von $f_1, \cdots, f_{m-1}$ und der ξ_i ist.

Die $P_1, \cdots, P_\alpha$ genügen infolgedessen, wie wir nun zeigen werden, einer Gleichung α^{ter} Ordnung, deren Koeffizienten rationale Formen der Unbestimmten von $f_1, \cdots, f_{m-1}$ sind. Es sei p irgend eine Linearform der $x_1, \cdots, x_m$ und bezeichne $P_i \times p$ die Linearinvariante von P_i und p. Ist ferner q irgend eine Form von kleinerer Ordnung als Θ, so bezeichne

$$q \times \Theta$$

die Polarform von q in bezug auf Θ. Es ist dann identisch

$$p^\alpha \times \Theta = P_1 \times p \cdot P_2 \times p \cdots P_\alpha \times p,$$

$$\frac{n p^{\alpha-1} \times \Theta}{p^\alpha \times \Theta} = \frac{P_1}{P_1 \times p} + \frac{P_2}{P_2 \times p} + \cdots + \frac{P_\alpha}{P_\alpha \times p},$$

$$\frac{(n)_2 p^{\alpha-2} \times \Theta}{p^\alpha \times \Theta} = \frac{P_1 \cdot P_2}{P_1 \times p \cdot P_2 \times p} + \frac{P_1 \cdot P_3}{P_1 \times p \cdot P_3 \times p} + \cdots \text{ etc.},$$

mithin sind die α Werte

$$H = \frac{P_i}{P_i \times p}$$

Wurzeln der Gleichung

$$p^\alpha \times \Theta \cdot H^\alpha - n \cdot p^{\alpha-1} \times \Theta \cdot H^{\alpha-1} + (n)_2 \cdot p^{\alpha-2} \times \Theta \cdot H^{\alpha-2} - \cdots = 0.$$

Die Größe

$$f_m \times P_1^\mu \cdot f_m \times P_2^\mu \cdots f_m \times P_\alpha^\mu$$

ist von den Wurzeln der obigen Gleichung in symmetrischer Weise abhängig. Daher ist sie ein Polynom der Koeffizienten jener Gleichung, und, da sie von den $\xi_1, \cdots, \xi_m$ unabhängig ist, also ein Polynom der Unbestimmten von $f_1, \cdots, f_m$. Sie läßt sich übrigens berechnen, indem man für f_m Aronholdsche Symbole

$$r_1, r_2, \cdots, r_\alpha$$

einführt und obigen Wert symbolisch als

$$\sum (r_{i_1} \times P_1 \cdot r_{i_2} \times P_2 \cdots r_{i_\alpha} \times P_\alpha)$$

ansetzt, die Summation ausgedehnt über alle verschiedenen Permutationen der $r_1, \cdots, r_\alpha$. Man könnte auf diesem Wege auch eine Rekursionsformel

gewinnen für die Aronholdschen Symbole der Resultante von m Formen und ähnlichen später einzuführenden Bildungen.

Damit ist die Existenz der Resultantenform außer Zweifel gestellt. Es erübrigt nur noch zu erweisen, daß, wenn R die Resultante von m gegebenen Formen $u_1, \cdots, u_m$ bezeichnet und l eine gegebene Linearform ist, eine Zahl M und Formen $a_1, \cdots, a_m$ der x_i wie der Koeffizienten von u_i existieren, so daß $R \cdot l^M = a_1 u_1 + \cdots + a_m u_m$. Die genaue Ausführung dieses Beweises hat für uns wenig Wert, da späterhin für ihn keine Verallgemeinerung nötig wird. Wir können daher auf das ausgezeichnete Buch von J. König verweisen, in dem der Beweis streng durchgeführt ist. Hier sei nur der Ideengang skizziert. Zunächst werde durch fortgesetzte Elimination einzelner Variabler erwiesen, und zwar am einfachsten bei Annahme nicht homogener Variabler, daß überhaupt eine Form F der Koeffizienten von $u_1, \cdots, u_m$ existiert, für die es eine Identität der obigen Gestalt

$$F = a_1 u_1 + \cdots + a_m u_m$$

gibt. Alsdann erweise man die Irreduzibilität der Form F, welche diese Eigenschaft besitzt und von der niedrigsten Ordnung ist, und zwar einfach dadurch, daß man im obigen die u_i als Linearformen ihrer Koeffizienten, die $x_1, \cdots, x_m$ aber als Parameter betrachtet, so daß aus

$$G \cdot H = a_1 u_1 + \cdots + a_m u_m$$

sogleich folgt entweder

$$G = b_1 u_1 + \cdots + b_m u_m$$

oder

$$H = c_1 u_1 + \cdots + c_m u_m.$$

Schließlich zeige man, daß F teilbar sein muß durch die Resultante von $u_1, \cdots, u_m$, da ja $F = 0$, wenn in irgend einem Punkte $P = x_1 : x_2 : \cdots : x_m$ die u_i gleichzeitig verschwinden. Macht man dann durch Ansetzen von $l = 1$ die Beziehung $R = a_1 u_1 \cdots$ in den x_i homogen, so folgt die Behauptung.

Die Resultante ist offenbar, als Polynom der Koeffizienten irgend *einer* der Formen u_i betrachtet, in ein Produkt von Linearformen auflösbar, wie sogleich aus der benutzten Identität

$$R = f_m \times P_1^\mu \cdots f_m \times P_\alpha^\mu$$

ersichtlich ist. Dieselbe Identität zeigt auch die Richtigkeit der Relation

$$\text{Res.}(u_1, \cdots, u_{m-1}, g) \cdot \text{Res.}(u_1, \cdots, u_{m-1}, h) = \text{Res.}(u_1, \cdots, u_{m-1}, g \cdot h)$$

in leicht verständlicher Schreibweise.

3. Wir erweisen nun

Satz I. „Sind $u_1, u_2, \cdots, u_h$ h Formen, wobei

$$h \leqq m,$$

derart, daß die Resultante von $u_1, \cdots, u_h$ und $m-h$ lineare Formen mit unbestimmten Koeffizienten nicht identisch verschwindet, und besteht eine identische Beziehung

$$p_1 u_1 + p_2 u_2 + \cdots + p_h u_h = 0,$$

wo die $p_1, \cdots, p_h$ Formen darstellen, so gibt es Formen $q_{i,j}$ derart, daß identisch

$$q_{i,i} = 0,$$
$$q_{i,j} + q_{j,i} = 0,$$
$$p_i = q_{i,1} u_1 + q_{i,2} u_2 + \cdots + q_{i,h} u_h."$$

Der Nachweis von Satz I wird zunächst erbracht werden für den Fall $h = m$, später für $h < m$. Der Beweis des genannten besonderen Falles wird durch Induktion erbracht werden, und zwar indem wir den Satz verifizieren, wenn $h = m = 2$, und dann aus der vorausgesetzten Richtigkeit des Satzes für einen Wert $m = m'$ die Richtigkeit des Satzes auch für den Wert $m = m' + 1$ erschließen.

Es sei also $m = 2$ und angenommen

$$p_1 u_1 + p_2 u_2 = 0.$$

Wenn die Resultante von u_1 und u_2 nicht verschwindet, so haben u_1 und u_2 keine gemeinsamen Nullpunkte und folglich muß p_1 durch u_2, p_2 durch u_1 teilbar sein. Es sei

$$p_1 = u_2 \cdot \Theta,$$

also

$$p_2 = -u_1 \cdot \Theta,$$

alsdann genügt es $q_{1,2} = \Theta$, $q_{2,1} = -\Theta$ zu setzen, um Satz I für den Fall $h = m = 2$ zu verifizieren.

Es sei nun die Richtigkeit des Satzes angenommen, wenn h und m den Wert $m' - 1$ annehmen. Alsdann beweisen wir zunächst, daß, wenn h und m gleich m' sind, aus einer Beziehung

$$p_1 u_1 + \cdots + p_{m-1} u_{m-1} + p_m \cdot l = 0,$$

wo l eine Linearform ist, deren Resultante mit $u_1, \cdots, u_{m-1}$ nicht verschwindet, die Existenz von Größen $q_1, q_2, \cdots, q_{m-1}$ folgt derart, daß

$$p_m = q_1 l + q_2 u_2 + \cdots + q_{m-1} u_{m-1}.$$

Zu diesem Zwecke wählen wir irgend ein System von $m-1$ Linearformen

$$l_1, l_2, \cdots, l_{m-1},$$

deren Determinante mit l nicht verschwindet, und entwickeln die

$$p_1, p_2, \cdots, p_{m-1}, u_1, \cdots, u_{m-1}$$

nach Potenzprodukten der $l_1, l_2, \cdots, l_{m-1}$ und l. Indem wir dann noch die von l unabhängigen Glieder absondern, können wir schreiben

$$\begin{aligned} p_1 &= p_1' + l \cdot p_1'', \\ p_2 &= p_2' + l \cdot p_2'', \\ &\cdots\cdots \\ p_{m-1} &= p_{m-1}' + l \cdot p_{m-1}'', \\ u_1 &= u_1' + l \cdot u_1'', \\ &\cdots\cdots \\ u_{m-1} &= u_{m-1}' + l \cdot u_{m-1}''. \end{aligned}$$

Die p_i' und u_j' sind hier also homogene Formen der $l_1, \cdots, l_{m-1}$. Die Relation

$$p_1 u_1 + p_2 u_2 + \cdots + p_m \cdot l = 0$$

zerspaltet sich nach Einsetzung obiger Werte in die beiden anderen

$$p_1' u_1' + p_2' u_2' + \cdots + p_{m-1}' u_{m-1}' = 0$$

und

$$p_1'' u_1 + p_1' u_1'' + p_2'' u_2 + p_2' u_2'' + \cdots + p_m = 0.$$

Da nun nach der gemachten Voraussetzung der Satz I richtig ist im Bereiche von $m-1$ Veränderlichen, so folgt aus der vorletzten Relation die Existenz von Formen $q_{i,j}'$ derart, daß für jeden Wert des Index i

$$\begin{aligned} p_i' &= q_{i,1}' u_1' + q_{i,2}' u_2' + \cdots, \\ q_{i,j}' + q_{j,i}' &= 0, \\ q_{i,i}' &= 0. \end{aligned}$$

Danach ist der Wert von

$$p_1' u_1'' + p_2' u_2'' + \cdots = q_{1,j}' u_j' \cdot u_1'' + q_{2,j}' u_j' \cdot u_2'' + \cdots$$

oder auch (da $q_{i,j}' + q_{j,i}' = 0$)

$$= \sum q_{i,j}' \cdot (u_j' u_i'' - u_i' u_j'')$$

$$i = 1, 2, \cdots, m-1$$

$$j = 1, 2, \cdots, m-1,$$

wo die Summation über alle Wertsysteme von i, j, in denen $i < j$, auszudehnen ist.

Nun war

$$u_j' + l \cdot u_j'' = u_j,$$

sonach ist

$$u_j' u_i'' - u_i' u_j'' = u_j \cdot u_i'' - u_i \cdot u_j''$$

und es zeigt sich somit aus der zweiten der obigen Relationen, daß Formen $q_1, \cdots, q_{m-1}$, für welche $p_m = q_1 u_1 + \cdots + q_{m-1} u_{m-1}$ ist, wirklich existieren.

Auch aus der Gleichung

$$p_1 u_1 + p_2 u_2 + \cdots + p_{m-1} u_{m-1} + p_m \cdot l^n = 0$$

folgt die Existenz solcher Formen q. Denn nach dem, was eben bewiesen, folgt zum mindesten die Existenz von $r_1, r_2, \cdots, r_{m-1}$, so daß

$$r_1 u_1 + r_2 u_2 + \cdots + r_{m-1} u_{m-1} + p_m \cdot l^{n-1} = 0$$

und auf diese Beziehung läßt sich derselbe Schluß wiederum anwenden und so immerfort.

Wir gehen nun zur ursprünglich gegebenen Beziehung zurück:

$$p_1 u_1 + p_2 u_2 + \cdots + p_m u_m = 0.$$

Wir wählen irgend eine Linearform l, deren Resultante mit $u_1, u_2, \cdots, u_{m-1}$ nicht verschwindet. Da die Resultante von $u_1, u_2, \cdots, u_m$ nicht verschwindet, so gibt es eine Zahl M derart, daß

$$l^M = s_1 \cdot u_1 + s_2 \cdot u_2 + \cdots + s_m \cdot u_m.$$

Somit ist

$$s_m p_1 u_1 + s_m p_2 u_2 + \cdots + s_m p_{m-1} u_{m-1} = p_m (s_1 u_1 + s_2 u_2 + \cdots - l^M)$$

oder

$$(s_m p_1 - p_m s_1) u_1 + (s_m p_2 - p_m s_2) u_2 + \cdots + p_m \cdot l^M = 0.$$

Es folgt also die Existenz von Formen $q_1, q_2, \cdots, q_{m-1}$, derart, daß

$$p_m = q_1 u_1 + q_2 u_2 + \cdots + q_{m-1} u_{m-1}.$$

Sobald also Satz I im Bereiche von $m-1$ Variablen gilt, folgt aus der Beziehung

$$p_1 u_1 + \cdots + p_m u_m = 0,$$

in welcher die Resultante von $u_1, \cdots, u_m$ nicht verschwindet, die obige Gleichung für p_m, welches auch die Ordnungen der $u_1, \cdots, u_m$ sein mögen. Daraus zeigt sich aber, daß auch aus

$$p_1 u_1 + \cdots + p_h u_h = 0,$$

wenn $h < m$, und die Resultante von $u_1, \cdots, u_h$ mit $m-h$ Linearformen nicht identisch verschwindet, eine Beziehung $p_h = q_1 u_1 + \cdots + q_{h-1} u_{h-1}$ folgt. Denn sind $g_1, g_2, \cdots, g_{m-h}$ irgend $m-h$ bestimmte Linearformen, deren Resultante mit $u_1, \cdots, u_h$ nicht verschwindet, ist ferner t irgend eine Form, deren Resultante mit $u_1, \cdots, u_{h-1}$ und den g_i nicht verschwindet, und ist n eine Zahl größer als die Ordnung von p_h, so folgt aus

$$p_1 u_1 + \cdots + p_h u_h = 0:$$

$$p_1 \cdot t \cdot u_1 + \cdots + p_{h-1} \cdot t \cdot u_{h-1} + p_h \cdot t \cdot u_h + 0 \cdot g_1^n + 0 \cdot g_2^n + \cdots = 0.$$

Mithin folgt, nach dem oben Bewiesenen, die Existenz von Formen $q_1, \cdots, q_{m-1}$, derart, daß

$$p_h = q_1 u_1 + \cdots + q_{h-1} u_{h-1} + q_{h+1} g_1^n + q_{h+2} \cdot g_2^n + \cdots$$

Die $q_{h+1}, q_{h+2}, \cdots$ müssen aber identisch 0 sein, wegen der Höhe der Zahl n.

Satz I ist damit im wesentlichen bewiesen, denn es ist nun leicht, die Werte der $q_{i,j}$ festzulegen. Sei $p_1 u_1 + \cdots + p_m u_m = 0$. Wir bestimmen Formen $Q_1, \cdots, Q_{m-1}$ derart, daß

$$p_m = Q_1 u_1 + \cdots + Q_{m-1} u_{m-1}$$

und setzen

$$q_{m,j} = Q_j, \quad q_{m,m} = 0.$$

Alsdann setzen wir diesen Wert von p_m in die obige Relation ein und ordnen dieselbe um, so daß sich ergibt

$$u_1(p_1 + q_{m,1} u_m) + u_2(p_2 + q_{m,2} u_m) + \cdots + u_{m-1}(p_{m-1} + q_{m,m-1} u_m) = 0.$$

Jetzt bestimmen wir wieder die Formen $R_1, R_2, \cdots, R_{m-2}$ derart, daß

$$p_{m-1} + q_{m,m-1} u_m = R_1 u_1 + R_2 u_2 + \cdots + R_{m-2} u_{m-2}$$

und setzen

$$q_{m-1,j} = R_j, \; q_{m-1,m-1} = 0,$$

$$q_{m-1,m} = - q_{m,m-1}.$$

So fahren wir fort. Es zeigt sich daraus die Richtigkeit des Satzes I einfach auf arithmetischem Wege.

Die Bedingung $h = m$ ist, wie wir jetzt sehen können, ganz überflüssig. Für kleinere Werte von h ist Satz I a fortiori richtig.

4. Ehe wir nun, auf Satz I fußend, weitergehen, wollen wir eine Bezeichnung einführen, welche Beziehungen wichtiger Art, die häufig wiederkehren, zweckmäßig abkürzend zum Ausdruck bringen wird. Es sei $f(R)$ irgend eine Funktion einer ganzen Zahl R, alsdann definieren wir einen Operator Δ_a durch die Gleichung $\Delta_a f(R) = f(R) - f(R-a)$. Ferner bezeichnen wir die Anzahl der Koeffizienten einer Form R^{ter} Ordnung im Bereiche von m Variablen mit $\varphi(R)$. Es ist also

$$\varphi(R) = \frac{(R+1)(R+2)\cdots(R+m-1)}{1 \cdot 2 \cdots (m-1)}.$$

Schließlich wollen wir, wenn $u_1, u_2, \cdots, u_h$ irgendwelche gegebene Formen sind, die Mannigfaltigkeit oder Anzahl der Konstanten, welche die Involution von Formen R^{ter} Ordnung hat, der die Multipla von u_1 oder $u_2 \cdots$ oder u_h angehören, mit

$$\varphi(R) - H(u_1, u_2, \cdots, u_h)(R)$$

bezeichnen, so daß also

$$H(u_1, u_2, \cdots, u_h)(R)$$

die Anzahl der linearen Bedingungen angibt, welchen die Koeffizienten einer Form R^{ter} Ordnung genügen müssen, damit eine solche Form der oben beschriebenen Involution angehöre.

5. Nach diesen Festsetzungen lautet

Satz II: „Die Anzahlfunktion

$$H(u_1, u_2, \cdots, u_h)(R)$$

ist $= \Delta_{a_1}\Delta_{a_2}\cdots\Delta_{a_h}\varphi(R)$, wenn die Resultante von $u_1, u_2, \cdots, u_h$ und $m-h$ Linearformen nicht identisch verschwindet, die $a_1, \cdots, a_h$ die Ordnungen der $u_1, \cdots, u_h$ angeben, und $R > a_1 + a_2 + \cdots + a_h - m$.

Ist aber unter denselben Bedingungen

$$R = a_1 + a_2 + \cdots + a_h - m,$$

so ist $H(u_1, \cdots, u_2)(R)$ um eins größer oder kleiner als der obige Wert, je nachdem $m-h$ gerade oder ungerade ist."

Der Beweis dieses Satzes wird durch Induktion erbracht. Sei zunächst $h = 1$. Alsdann besteht die Involution von Formen R^{ter} Ordnung, welche Multipla von u_1 sind, aus allen Formen

$$p \cdot u_1,$$

wo p irgend eine Form $(R-a_1)^{\text{ter}}$ Ordnung. Die Mannigfaltigkeit dieser Involution ist sonach $\varphi(R-a_1)$, wenn $R \geqq a_1$, und 0, wenn $R < a_1$. Nun ist aber $\varphi(R-a_1) = 0$, wenn $R - a_1 = -1$ oder $= -2 \cdots$ oder $= -m+1$. Dagegen ist $\varphi(R-a_1) = (-1)^{m-1}$, wenn $R - a_1 = -m$. Mit anderen Worten: $H(u_1)(R)$ ist $= \Delta_{a_1}\varphi(R)$, wenn $R > a_1 - m_1$ und $= \Delta_{a_1}\varphi(R) + (-1)^{m-1}$, wenn $R = a_1 - m_1$, Satz II also richtig, wenn $h = 1$.

Die Richtigkeit des Satzes II sei nun angenommen für einen beliebigen Wert von h, wir müssen dann zeigen, daß daraus die Richtigkeit von Satz II für einen um die Einheit größeren Wert von h folgt.

Zu diesem Zwecke bedienen wir uns eines sehr einfachen und augenscheinlichen, jedoch trotzdem häufig anwendbaren Hilfssatzes. Derselbe besagt, daß die Involution von Formen R^{ter} Ordnung, welche von beliebig gegebenen Formen R^{ter} Ordnung

$$f_1, f_2, \cdots, f_u$$

gebildet wird, die Mannigfaltigkeit

$$u - v$$

hat, wo v die Anzahl der voneinander linear independenten Beziehungen der Gestalt

$$c_1 f_1 + c_2 f_2 + \cdots + c_u f_u = 0$$

angibt. Danach ist die Mannigfaltigkeit der von den Multipla der $u_1, \cdots, u_h$ gebildeten Involution gleich der Mannigfaltigkeit der von den Multipla von $u_1, \cdots, u_{h-1}$ gebildeten Involution, vermehrt um die Mannigfaltigkeit der Multipla von u_h und vermindert um die Anzahl der linear independenten Beziehungen der Gestalt

$$p_1 u_1 + \cdots + p_{h-1} u_{h-1} = p_h u_h.$$

Die beiden ersteren Mannigfaltigkeiten lassen sich leicht bestimmen, da Satz II für $h-1$ Formen Geltung haben soll. Die letztere Mannigfaltigkeit ergibt sich aus Satz I, da aus der obigen Beziehung folgt

$$p_h = q_1 u_1 + q_2 u_2 + \cdots + q_{h-1} u_{h-1}.$$

Wenn $R > a_1 + a_2 + \cdots + a_h - m$, ist die Mannigfaltigkeit der Involution $p_1 u_1 + \cdots + p_{h-1} u_{h-1}$, nämlich $\varphi(R) - H(u_1, \cdots, u_{h-1})(R)$, nach der gemachten Annahme gleich $\varphi(R) - \Delta_{a_1} \cdots \Delta_{a_{h-1}} \varphi(R)$. Die Mannigfaltigkeit der Multipla von u_h ist $= \varphi(R - a_h)$. Ferner wenn $R - a_h$, welches die Ordnung von p_h ist, $> a_1 + \cdots + a_{h-1} - m$ ist, so ist die Anzahl der linear independenten Relationen der Gestalt $p_1 u_1 + \cdots + p_h u_h = 0$ nach Satz I gleich der Mannigfaltigkeit der Formen p_h, die der Involution von Formen $(R - a_h)^{\text{ter}}$ Ordnung der Multipla von $u_1, \cdots, u_{h-1}$ angehören, also $= \varphi(R - a_h) - H(u_1, \cdots, u_{h-1})(R - a_h)$; und nur wenn $R - a_h = a_1 + \cdots + a_{h-1} - m$ ist, ist letztere Anzahl

$$= \varphi(R - a_h) - H(u_1, \cdots, u_{h-1})(R - a_h) + (-1)^{m-h}.$$

Also ist

$$\varphi(R) - H(u_1, \cdots, u_h)(R) = \varphi(R) - \Delta_{a_1} \cdots \Delta_{a_{h-1}} \varphi(R) + \Delta_{a_1} \cdots \Delta_{a_{h-1}} \varphi(R - a_h),$$

wenn

$$R > a_1 + \cdots + a_h - m,$$

und um $(-1)^{m-h}$ kleiner, wenn $R = a_1 + \cdots + a_h - m$. Danach ist schließlich

$$H(u_1, \cdots, u_h)(R) = \Delta_{a_1} \cdots \Delta_{a_{h-1}} \Delta_{a_h} \varphi(R),$$

wenn

$$R > a_1 + \cdots + a_h - m$$

und

$$\Delta_{a_1} \cdots \Delta_{a_h} \varphi(R) + (-1)^{m-h},$$

wenn

$$R = a_1 + \cdots + a_h - m.$$

Satz II also damit verifiziert.

6. Satz II wenden wir zunächst für den Fall

$$h = m$$

an. $\Delta_{a_1} \cdots \Delta_{a_h} \varphi(R)$ ist dann $= 0$. Jede beliebige Form F, deren Ordnung $> a_1 + a_2 + \cdots + a_m - m$ ist, läßt sich danach in der Gestalt

$$p_1 u_1 + \cdots + p_m u_m$$

darstellen, wenn die Resultante der u_i nicht verschwindet. Die Formen der Ordnung

$$a_1 + \cdots + a_m - m$$

dagegen haben genau eine Bedingung zu erfüllen, wenn sie in dieser Weise darstellbar sein sollen. Nach den Bezeichnungen der Invariantenrechnung und der Begriffsbildung von Rosanes kann man sagen, daß eine

ganz bestimmte Form Ω in kontragredienten Variablen und der Ordnung $a_1 + \cdots + a_m - m$ existiert, zu der alle Formen derselben Ordnung, welche Multipla von einem der u_i sind, konjugiert sind, zu der also die $u_1, \cdots, u_m$ selbst sämtlich apolar sind. Wir können dann den Satz aufstellen:

Satz III. „Wenn die Resultante von $u_1, \cdots, u_m$ nicht verschwindet, so ist die notwendige und hinreichende Bedingung für die Darstellbarkeit einer Form F durch $p_1 u_1 + \cdots + p_m u_m$ die Apolarität von F zu Ω."

Wir beweisen Satz III durch den folgenden Prozeß. Zuerst zeigen wir, daß Satz III zutrifft, wenn die $u_1, \cdots, u_m$ sämtlich Potenzen von Linearformen sind. Alsdann weisen wir nach, daß aus der Annahme der Richtigkeit von Satz III, wenn k der u_i Potenzen von Linearformen sind, auch die Richtigkeit des Satzes folgt, wenn nur $k-1$ der Formen u_i solche Potenzen sind.

Es seien $u_i = l^{a_i}$, wo $l_1, l_2, \cdots, l_m$ Linearformen, deren Determinante nicht verschwindet, welche also als die unabhängigen Variablen gedeutet werden können. Demgemäß bezeichnen wir l_i mit x_i und führen ein System kontragredienter Variablen $y_1, \cdots, y_m$ ein, welche mit den $x_1, \cdots, x_m$ durch die Gleichung

$$x_1 y_1 + \cdots + x_m y_m = l$$

verbunden sein mögen. Nach dem Ergebnisse des Satzes II gibt es eine einzige Form Ω der Ordnung $a_1 + a_2 + \cdots + a_m - m$, zu der die $x_i^{a_i}$ sämtlich apolar sind. Da $y_1^{a_1-1} \cdot y_2^{a_2-1} \cdots y_m^{a_m-1}$ eine solche Form ist, so muß Ω mit diesem Ausdruck, abgesehen von einem numerischen Faktor, identisch sein. Satz III sagt für das vorgeschlagene System der $u_1, \cdots, u_m$ aus, daß die hinreichende Bedingung dafür, daß eine Form F in der Gestalt

$$p_1 x_1^{a_1} + p_2 x_2^{a_2} + \cdots + p_m x_m^{a_m}$$

darstellbar sei, in der Apolarität von F zu Ω ruhe.

Es sei nun $x_1^{b_1} \cdot x_2^{b_2} \cdots x_m^{b_m}$ irgend ein Potenzprodukt. Die Polare desselben in bezug auf $y_1^{a_1-1} \cdot y_2^{a_2-1} \cdots y_m^{a_m-1}$ ist, abgesehen von einem numerischen Faktor, identisch mit $y_1^{a_1-b_1-1} \cdot y_2^{a_2-b_2-1} \cdots y_m^{a_m-b_m-1}$ und nur $= 0$, wenn eines der b_i zum mindesten gleich dem entsprechenden a_i. Somit kann auch eine beliebige Summe von Potenzprodukten der obigen Gestalt nur zu Ω apolar sein, wenn in jedem einzelnen der Potenzprodukte der Summe mindestens einer der Exponenten gleich oder größer ist, als das entsprechende a_i. Dann ist diese Summe von Potenzprodukten darstellbar in der Gestalt

$$p_1 x_1^{a_1} + \cdots + p_m x_m^{a_m}.$$

Jede Form F ist aber ausdrückbar als eine Summe von Potenzprodukten. Somit ist die Apolarität von F zu Ω in der Tat hinreichende Bedingung der Darstellbarkeit von F in der Gestalt $p_1 x_1^{a_1} + \cdots + p_m x_m^{a_m}$.

Wir gehen nun zu dem Induktionsschlusse über, wie er vorhin charakterisiert war. Es seien $u_1, \cdots, u_m$ m Formen, deren Resultante nicht verschwindet, $k-1$ derselben seien Potenzen von Linearformen und u_1 sei keine solche Potenz. Es sei l irgend eine Linearform, deren Resultante mit $u_2, u_3, \cdots, u_m$ nicht verschwindet. Ist die positive ganze Zahl M groß genug gewählt, so gibt es Formen $s_1, s_2, \cdots, s_m$, derart, daß

$$l^M = s_1 u_1 + s_2 u_2 + \cdots + s_m u_m.$$

Die Form Ω, welche zu dem System

$$l^M, u_2, u_3, \cdots, u_m$$

gehört, hat die Ordnung $M + a_2 + \cdots + a_m - m$ und sei mit $\Omega(l^M, u_2, \cdots, u_m)$ bezeichnet. Dieselbe ist apolar zu $u_2, u_3, \cdots, u_m$ und l^M, also auch zu $s_1 \cdot u_1$. s_1 ist nicht apolar zu $\Omega(l^M, \cdots, u_m)$, denn sonst wäre, nach der gemachten Annahme, da die Reihe $l^M, \cdots, u_m$ k Potenzen von Linearformen enthält, s_1 darstellbar in der Gestalt $p_1 l^M + p_2 u_2 + \cdots + p_m u_m$, und dies würde wegen des offenbaren identischen Verschwindens von p_1 und der Gleichung $l^M = s_1 u_1 + s_2 u_2 + \cdots$ damit in Widerspruch stehen, daß die Resultante von l und $u_2, \cdots, u_m$ nicht verschwinden soll. $s_1 \times \Omega(l^M, u_2, \cdots, u_m)$, wie ich die Polare von s_1 in bezug auf $\Omega(l^M \cdots)$ bezeichnen will, ist eine Form der Ordnung $a_1 + \cdots + a_m - m$, apolar zu $u_1, u_2, \cdots, u_m$, also bis auf einen konstanten Faktor identisch mit $\Omega(u_1, u_2, \cdots, u_m)$. In Wahrheit besteht die Relation

$$s_1 \times \Omega(s_1 \cdot u_1, u_2, \cdots, u_m) = \operatorname{Res}(s_1, u_2, \cdots, u_m) \cdot \Omega(u_1, \cdots, u_m).$$

Doch kommt es auf den Wert des konstanten Faktors für die zu machende Schlußfolgerung gar nicht an. Sei nun F irgend eine Form apolar zu $\Omega(u_1, u_2, \cdots, u_m)$. Da identisch

$$s_1 \cdot F \times A = F \times (s_1 \times A),$$

welches auch die Form A sei, so ist, abgesehen von einem konstanten Faktor,

$$s_1 \cdot F \times \Omega(l^M, u_2, \cdots, u_m) = F \times \Omega(u_1, u_2, \cdots, u_m) = 0.$$

$s_1 \cdot F$ ist also apolar zu $\Omega(l^M, u_2, \cdots, u_m)$ und daher, nach der gemachten Annahme, darstellbar in der Gestalt

$$s_1 F = p_1 l^M + p_2 \cdot u_2 + \cdots + p_m \cdot u_m,$$

was wegen $l^M = s_1 \cdot u_1 + s_2 \cdot u_2 + \cdots$ zu einer Beziehung der Art

$$s_1 (F - p_1 u_1) = q_2 \cdot u_2 + \cdots + q_m \cdot u_m$$

führt. Nun verschwindet aber die Resultante von $s_1, u_2, \cdots, u_m$ nicht, da ja die Beziehung besteht

$$\operatorname{Res}(l^M, u_2, \cdots, u_m) = \operatorname{Res}(s_1, u_2, \cdots, u_m) \cdot \operatorname{Res}(u_1, \cdots, u_m).$$

Somit folgt aus obiger Relation nach Satz I die andere

$$F - p_1 u_1 = r_2 u_2 + \cdots + r_m u_m,$$

wo die $r_2, \cdots, r_m$ Formen. Jede zu $\Omega(u_1, \cdots u_m)$ apolare Form ist also in der Gestalt $t_1 u_1 + t_2 u_2 + \cdots$ darstellbar, wie Satz III behauptet.

7. Um einen Weg zur genaueren Berechnung und Charakterisierung von Ω zu zeigen, wenden wir Satz III für den Fall $h = m - 1$,

$$R = a_1 + a_2 + \cdots + a_{m-1} - m$$

an. Da

$$\Delta_{a_1} \Delta_{a_2} \cdots \Delta_{a_{m-1}} \varphi(R) = a_1 \cdot a_2 \cdots a_{m-1},$$

so sagt uns Satz II, daß, wenn die Resultante von $u_1, u_2, \cdots, u_{m-1}$ und einer Linearform nicht identisch verschwindet, es eine

$$(a_1 \cdot a_2 \cdots a_{m-1} - 1)\text{-}$$

fache Bedingung für eine Form F der Ordnung $a_1 + a_2 + \cdots a_{m-1} - m$ sei, in der Gestalt

$$p_1 u_1 + \cdots + p_{m-1} u_{m-1}$$

darstellbar zu sein. Sind die Koeffizienten von $u_1, \cdots, u_{m-1}$ lauter unbestimmte Größen, so zerfällt die Resultante von $u_1, \cdots, u_{m-1}$ und einer Linearform l mit den unbestimmten Koeffizienten $y_1, \cdots, y_m$ in $a_1 \cdot a_2 \cdots a_{m-1}$ Linearformen von $y_1, \cdots, y_m$. Denn einerseits ist es nach Satz II eine $a_1 \cdots a_{m-1}$-fache Bedingung für eine Form F von genügend hoher Ordnung, in der Gestalt

$$F = p_1 u_1 + \cdots + p_{m-1} u_{m-1}$$

darstellbar zu sein. Andererseits muß F für alle Wertsysteme verschwinden, welche $u_1, \cdots, u_{m-1}$ zugleich zu Null machen. Und, wie man aus dem besonderen Falle, daß die $u_1, \cdots, u_{m-1}$ in lauter Linearfaktoren zerfallen, ersehen kann, haben die $u_1, \cdots, u_{m-1}$ für unbestimmte Werte ihrer Koeffizienten zum mindesten

$$a_1 \cdots a_{m-1}$$

distinkte Wertsysteme gemein, für die sie verschwinden. Daher ist $a_1 \cdots a_{m-1}$ die genaue Zahl der gemeinsamen „Nullpunkte" von

$$u_1, \cdots, u_{m-1}.$$

Es sei

$$\operatorname{Res}(u_1, \cdots, u_{m-1}, l) = A_1 A_2 \cdots A_n$$

für

$$n = a_1 \cdot a_2 \cdots a_{m-1}.$$

Soll F in der Gestalt $p_1 u_1 + \cdots + p_{m-1} u_{m-1}$ darstellbar sein, so muß F jeden der Punkte $A_1, A_2, \cdots, A_n$ enthalten, und da ersteres nur eine $(n-1)$-fache Bedingung ist, so müssen (nach den Ausführungen von Hesse, Bonnet, Rosanes u. a.) die Potenzen

$$A_1^r, A_2^r, \cdots, A_n^r,$$

wo

$$r = a_1 + a_2 + \cdots + a_{m-1} - m$$

ist, zum mindesten durch *eine* lineare Bedingung verknüpft sein. Es seien nun $c_1, \cdots, c_n$ solche Konstanten, daß

$$c_1 \cdot A_1^r + c_2 \cdot A_2^r + \cdots + c_n \cdot A_n^r = 0.$$

Alsdann ist, wie man leicht sieht,

$$W = c_1 \frac{A_1^{r+a_m}}{u_m \times A_1^{a_m}} + c_2 \frac{A_2^{r+a_m}}{u_m \times A_2^{a_m}} + \cdots$$

eine Form der Variablen $y_1, \cdots, y_m$ von der Ordnung

$$a_1 + a_2 + \cdots + a_m - m,$$

zu der $u_1, u_2, \cdots, u_m$ sämtlich apolar sind. Um dieselbe von Nennern zu befreien, multiplizieren wir sie mit

$$u_m \times A_1^{a_m} \cdot u_m \times A_2^{a_m} \cdots = \mathrm{Res}\,(u_1, \cdots, u_m).$$

Diese Form ist es, die wir mit Ω identifizieren. Ω ist also eine kontragrediente Form der Ordnung $a_1 + \cdots + a_m - m$, deren Koeffizienten von den unbestimmt gedachten Koeffizienten der $u_1, \cdots, u_m$ rational und ganz abhängen und die z. B. die Koeffizienten von u_m in der Ordnung

$$a_1 \cdot a_2 \cdots a_{m-1} - 1$$

enthält. Ω wird die $(a_1 + \cdots + a_m - m)^{\text{te}}$ Potenz einer Linearform A, wenn die Resultante von $u_1, u_2, \cdots, u_m$ verschwindet, wobei A der dann den $u_i = 0$ gemeinsame Punkt ist. Haben aber $u_1, \cdots, u_m$ mehr als *einen* Punkt gemeinsam, oder berühren sich die $u_1 = 0, \cdots, u_m = 0$ in einem gemeinsamen Punkte, so verschwindet Ω identisch.

Ist D die Funktionaldeterminante der $u_1, u_2, \cdots, u_m$, so ist

$$D \times \Omega = \mathrm{Res},$$

wo Res die Resultante von $u_1, u_2, \cdots, u_m$ bezeichnet. Wenn nämlich Res verschwindet, so ist, abgesehen von einem konstanten Faktor,

$$\Omega = A^{a_1 + \cdots + a_m - m};$$

andererseits, wenn $u_1, \cdots, u_m$ in A verschwinden, enthält auch die Funktionaldeterminante D den Punkt A. $D \times \Omega$ ist also immer 0, wenn $\mathrm{Res} = 0$. Nun enthält $D \times \Omega$ die Koeffizienten von u_m z. B. genau zur selben Ordnung wie Res. $D \times \Omega$ ist also nicht bloß teilbar durch Res, sondern ist gleich einem numerischen Multiplum von Res. Daß $D \times \Omega$ nicht identisch verschwindet, ergibt sich sogleich aus dem speziellen Falle

$$u_1 = x_1^{a_1}, \cdots, u_m = x_m^{a_m}, \; D = x_1^{a_1 - 1} \cdot x_2^{a_2 - 1} \cdots x_m^{a_m - 1},$$
$$\Omega = y_1^{a_1 - 1} \cdots y_m^{a_m - 1}.$$

Man ersieht übrigens aus obigem, daß die notwendige und hinreichende Bedingung für die Existenz einer Relation

$$D = p_1 u_1 + \cdots + p_m u_m$$

das Verschwinden von Res $(u_1, \cdots, u_m)$ ist.

Es wäre wohl möglich, obige nur kurz angedeutete Beziehungen zwischen D, Ω, Res $(u_1, \cdots, u_m)$ und der Gleichung $c_1 \cdot A_1^r + \cdots + c_n \cdot A_n^r = 0$ etc. bedeutend zu vertiefen. Doch liegen die Ziele dieser Arbeit nach einer so ganz anderen Richtung, daß es unstatthaft erscheint, die erwähnte Linie der Forschung hier noch weiter zu verfolgen.

8. Ein Wertsystem $x_1 : x_2 : \cdots : x_m$ nannten wir einen Punkt. Die Gesamtheit aller solcher Punkte heiße der „Raum" $x_1, \cdots, x_m$. Sind die $x_1 : x_2 : \cdots : x_m$ durch funktionale Beziehungen voneinander abhängig gemacht, etwa dergestalt:

$$\begin{aligned} x_{i+1} &= f(x_1, \cdots, x_i), \\ x_{i+2} &= g(x_1, \cdots, x_i), \\ &\cdots\cdots\cdots \\ x_m &= h(x_1, \cdots, x_i), \end{aligned}$$

so heißt die Gesamtheit der solchergestalt zusammengefaßten Punkte ein „Gebilde". Für uns genügt es, die $f, g, \cdots, h$ als *algebraische* Funktionen anzunehmen und im übrigen darauf hinzuweisen, daß bei einer Erweiterung des Bereiches, aus dem die $f, g, \cdots, h$ gewählt sind, wenn nur der Resultantenbegriff sich auch entsprechend erweitern läßt, unsere gesamten Ergebnisse sich fast ohne weiteres übertragen lassen auf den größeren Funktionsbereich.

Eine durch die Gleichungen

$$f_1 = 0,\ f_2 = 0,\ \cdots,\ f_h = 0,$$

wo $f_1, \cdots, f_h$ Formen sind, definierte Mannigfaltigkeit von Punkten werden wir ein „algebraisches Gebilde" oder genauer eine „Konfiguration" von algebraischen Gebilden nennen. Es wird nun unsere Aufgabe sein, zu zeigen, daß eine solche Konfiguration sich in eindeutiger Weise darstellen läßt, als eine Nebeneinanderlagerung von algebraischen derartigen Konfigurationen besonderer Art.

9. Jede Form F läßt sich in eindeutiger Weise als Produkt irreduzibler Formen darstellen, wie sich aus den Elementen der Algebra in bekannter einfacher Weise folgern läßt. Es sei F eine irreduzible Form, F' eine zweite. Wir bilden die Resultante von F, F' und $m-2$ Linearformen $l_1, \cdots, l_{m-2}$, deren Koeffizienten durchweg Unbestimmte sind und mit

$$\begin{matrix} y_{1,1}, \cdots, y_{1,m} \\ \cdots\cdots\cdots \\ y_{m-2,1}, \cdots, y_{m-2,m} \end{matrix}$$

bezeichnet sein mögen. Dieselbe ist eine Form der $y_{i,j}$ und daher darstellbar als Produkt

$$\mathrm{Res}(F, F', l_1, \cdots, l_{m-2}) = G_1^{a_1} \cdot G_2^{a_2} \cdots G_k^{a_k},$$

wo die G_i sämtlich irreduzible Formen der $y_{i,j}$ sind. Es sei Γ irgend eine der irreduziblen Formen G. Alsdann definieren wir einen Bereich von Formen $F, F', F'', \cdots$ durch die Festsetzung, daß er nur und alle die Formen umfassen soll, deren Resultante mit F und $l_1, \cdots, l_{m-2}$ als Form der $y_{i,j}$ aufgefaßt durch Γ teilbar ist. Von diesem Bereich werden wir zeigen, daß das Verschwinden seiner Formen

$$F = 0, F' = 0, F'' = 0, \cdots$$

ein Gebilde definiert, welches niemals auf dem Produkt zweier Formen $A \cdot B$ gelegen sein kann, ohne daß einer der Faktoren A oder B es vollständig enthalten, und das wir daher als irreduzibles algebraisches Gebilde bezeichnen werden.

Die Resultante $\mathrm{Res}(F, F', l, \cdots, l_{m-2})$, als Form der $y_{m-2,1}, \cdots, y_{m-2,m}$ allein betrachtet, läßt sich in ein Produkt von lauter Linearfaktoren zerlegen, dasselbe trifft daher zu für jeden der Teiler der Resultante, also auch für Γ. Schreiben wir

$$\Gamma = (b_1 y_{m-2,1} + b_2 y_{m-2,2} + \cdots)(c_1 y_{m-2,1} + c_2 y_{m-2,2} + \cdots) \cdots,$$

wo die $b_1, b_2, \cdots, c_1, c_2, \cdots$ irrationale Funktionen der $y_{i,j}$ $(i \leq m-3)$ sein werden, so bestimmen $b_1 : b_2 :$ etc. und $c_1 : c_2 :$ etc. Punkte, die zufolge der Bedeutung der Resultante die Formen $F, F', l_1, l_2, \cdots, l_{m-3}$ zugleich verschwinden machen. Es ist die Gesamtmannigfaltigkeit all dieser Punkte, für alle Wertsysteme der $y_{i,j}$ $(i \leq m-3)$, welche das algebraische Gebilde ausmachen, das der Untersuchung unterliegt. Nennen wir diese Punktmannigfaltigkeit C. Ist F'' irgend eine Form, die die betreffende Mannigfaltigkeit enthält, so muß die Resultante von F, F'', $l_1, l_2, \cdots, l_{m-2}$ den Faktor Γ haben, denn $F = 0$, $F'' = 0$, $l_1 = 0$, $l_2 = 0$, $\cdots, l_{m-2} = 0$ haben zum mindesten jene oben erwähnten Punkte $b_1 : b_2 \cdots$, $c_1 : c_2 \cdots$ etc. gemein. Andererseits, wenn die Resultante von F, F'', l_1, $\cdots, l_{m-2}$ den Faktor Γ hat, so muß F'' die Mannigfaltigkeit C enthalten. Gehört $A \cdot B$ der Menge der Formen an, welche für alle Punkte von C verschwinden, so muß die Resultante von $F, A \cdot B, l_1, l_2, \cdots, l_{m-2}$ den Faktor Γ enthalten. Die betreffende Resultante ist jedoch das Produkt der Resultanten von $F, A, l_1, \cdots, l_{m-2}$ und $F, B, l_1, \cdots, l_{m-2}$ und Γ ist irreduzibel. Mithin muß entweder die Resultante von $F, A, l_1, \cdots, l_{m-2}$ oder die von $F, B, l_1, \cdots, l_{m-2}$ durch Γ teilbar sein, also C entweder in A oder in B enthalten sein.

Die Punktmenge C hat mit $m-3$ beliebig gewählten Linearformen $l_1, \cdots, l_{m-3}$ Punkte gemein, wir sagen daher, C hat die Mannigfaltigkeit $m-2$, oder die Dimension $m-3$ oder die Stufe (oder Rang) 2.

Es sei f eine Form, welche C nicht enthalte. Das „Schnittgebilde" von $f=0$ und C wird dann wie folgt bestimmt.

Wir gehen aus von der Identität

$$\Gamma = (b_1 y_{m-2,1} + b_2 y_{m-2,2} + \cdots)(c_1 y_{m-2,1} + c_2 y_{m-2,2} + \cdots),$$

die wir $\Gamma = L_1 \cdot L_2 \cdots L_u$ schreiben, unter $L_1, \cdots, L_u$ die Linearfaktoren der $y_{m-2,i}$ verstanden. Indem wir nun wieder die Linearinvariante zweier kontragredienter Formen F, Φ derselben Ordnung symbolisch mit $F \times \Phi$ bezeichnen, definieren wir eine Zahl $\Delta = f \times L_1^r \cdot f \times L_2^r \cdots f \times L_u^r$, wo r die Ordnung von f bezeichnet.

Dieselbe ist, wie nach der schon früher benutzten Methode erweisbar, eine Form der unbestimmten Koeffizienten von $l_1, \cdots, l_{m-3}$, und verschwindet nur, wenn C, f und $l_1, \cdots, l_{m-3}$ einen Punkt gemeinsam haben. Δ kann als Form der Koeffizienten von $l_1, \cdots, l_{m-3}$ in seine irreduziblen Teiler zerlegt werden

$$= \Delta_1^{a_1} \Delta_2^{a_2} \cdots$$

Jedem der Δ_i entspricht dann ein „irreduzibles Gebilde" dritter Stufe, die Gesamtheit aller der Punkte, die $C, f, l_1, \cdots, l_{m-4}$ gemein sind, wenn die Koeffizienten von l_{m-3} als Parameter gedeutet werden. Enthält ein Produkt von Formen $A \cdot B$ das Δ_1 entsprechende Punktgebilde, so muß der wie oben konstruierte Schnitt von $C, A \cdot B$ und $l_1, \cdots, l_{m-3}$ den Faktor Δ_1 enthalten.

Und ist umgekehrt jener Schnitt teilbar durch Δ_1, so muß $A \cdot B$ das Δ_1 entsprechende Punktgebilde enthalten. Da nun der Schnitt in den von $C, l_1, \cdots, l_{m-3}, A$ und den von $C, l_1, \cdots, l_{m-3}, B$ zerfällt, Δ_1 aber irreduzibel ist, so muß entweder A oder B das Δ_1 entsprechende Punktgebilde enthalten. Darin beruht der Charakter der Irreduzibilität dieses Gebildes.

Auf diesem Wege kann man weitergehen und den Begriff des irreduziblen Gebildes n^{ter} Stufe definieren.

10. Satz IV. „Die durch das Nullsetzen von beliebig vielen Formen $f_1, f_2, \cdots, f_h$ definierte Punktmannigfaltigkeit läßt sich in eine endliche Zahl von irreduzibeln Gebilden zerspalten und zwar in eindeutiger Weise."

Um dieselben zu finden, zerspalten wir f_1 in seine irreduziblen Teiler und legen diejenigen in eine Gruppe G, welche jede der $f_2, \cdots, f_h$ teilen, die übrigen in eine andere Gruppe G'. Aus G' wählen wir irgend eine Form F, bringen irgend eine der sie nicht enthaltenden Formen f_i mit ihr zum Schnitt und bestimmen die irreduziblen Schnittgebilde von (F, f_i).

Alle diejenigen dieser Gebilde, welche in $f_2, \cdots, f_h$ enthalten sind, fügen wir der Gruppe G zu, aus den übrigen bilden wir eine Gruppe G''. So verfahren wir mit allen verschiedenen Formen von G'. Alsdann entnehmen wir G'' irgend ein Schnittgebilde zweiter Stufe, repräsentiert durch eine Form Φ, und bringen dasselbe zum Schnitt mit irgend einer der Formen f_i, welche es nicht enthält. Die entstehenden irreduziblen Gebilde dritter Stufe fügen wir entweder der Gruppe G zu, nämlich wenn alle f_i sie enthalten, oder einer anderen Gruppe G''', wenn dies nicht der Fall ist, und setzen dies Verfahren fort. Die Gruppe G wird schließlich alle und nur die gemeinsamen Punkte von $f_1 = 0, \cdots, f_h = 0$ enthalten und diese in irreduziblen Gebilden verschiedener Stufen zusammengefaßt. Auch ist klar, daß ein den $f_i = 0$ gemeinsames irreduzibles Gebilde der Gruppe G angehören muß. Somit ist die Behauptung des Satzes IV verifiziert.

Jedem irreduziblen Punktgebilde entsprach eine irreduzible Form von Unbestimmten $y_{i,j}$. Es ist klar, daß an Stelle der Linearformen l_i auch Formen höherer Ordnung mit unbestimmten Koeffizienten hätten in derselben Weise zur Verwendung gelangen können, die Schlüsse wären dadurch in keiner Weise beeinflußt worden. Dies ist wichtig, weil in Kap. IV eine Algebra definiert wird, die derartiger Formen höherer Ordnung als Hilfsformen wirklich bedarf. Andrerseits hätten wir unser Ziel auch erreichen können, indem wir auf die Variablen $x_1, \cdots, x_m$ eine lineare Transformation mit unbestimmten Koeffizienten $y_{i,j}$ ausführten und die Resultantenbildungen der Formen f_i in bezug auf den „Raum" einiger der neuen Variablen x_i benutzten; diese Methode ist nicht wesentlich von der hier benutzten verschieden, denn es macht keinen Unterschied, ob die obige Transformation erst ausgeführt wird und nachher einige der Variablen eliminiert werden, oder ob die Elimination ausgedehnt wird auf alle Variablen, nachdem lineare Beziehungen zwischen denselben statuiert sind. Die letzterwähnte Methode ist im Werke von J. König im Anschluß an die Kroneckersche Eliminationsmethode streng durchgeführt, weswegen hier darauf verwiesen sein mag.

11. Die Erwägungen, welche zu obigen Resultanten führten, lassen sich wiederholen, wenn von den Koeffizienten aller vorkommenden Formen die Ganzzahligkeit gefordert wird. Denn auch ganzzahlige Formen sind nur auf *eine* Weise in irreduzible Faktoren zerlegbar. Der Charakter des Irreduzibilitätsbegriffes ändert sich allerdings beim Übergang von Formen mit beliebig gegebenen Koeffizienten zu ganzzahligen Formen, da irreduzible ganzzahlige Formen unter dem Gesichtspunkte der Algebra mit beliebigen Koeffizienten reduzibel sein können. Dies ändert aber nichts an den Schlüssen des Satzes IV.

Die verschiedenen Teiler einer im Bereiche der ganzen Zahlen irre-

duziblen Form heißen „konjugiert". Nennen wir die Gesamtheit der Punkte, die eine Anzahl von ganzzahligen Formen $f_1, \cdots, f_h$ zu Null machen, die ganzzahlige Konfiguration $f_1 = 0, \cdots, f_h = 0$, so können wir sagen:

Satz V. „Jede ganzzahlige Konfiguration zerfällt in eine endliche Anzahl konjugierter irreduzibler Gebilde."

Oder wenn wir das Produkt von konjugierten irreduziblen Gebilden im Sinne der Algebra der ganzen Zahlen als irreduzibel auffassen:

„Jede ganzzahlige Konfiguration zerfällt in eine endliche Anzahl ganzzahliger irreduzibler Gebilde."

Kapitel II.

Über Moduln und Ideale im Raume $x_1, \cdots, x_m$.

12. Ein Bereich von Formen, dadurch gekennzeichnet, daß, wenn p und q ihm angehören und a und b beliebige Formen sind, auch $ap + bq$ ihm angehört, heißt ein *Modul.*

Ein Bereich von ganzzahligen Formen, dadurch gekennzeichnet, daß, wenn p und q ihm angehören und a und b beliebige ganzzahlige Formen sind, auch $ap + bq$ ihm angehört, heißt ein *Ideal.*

Die beiden Begriffe, welche wir soeben definiert haben, haben eine sehr langsame Entwicklung durchgemacht, und ihre hohe Bedeutung ist erst etwa in den letzten 40 Jahren erkannt worden. Im Keime ist der Idealbegriff bereits in den Schriften von Gauß enthalten. Gauß führte in seinem Werke „Disquisitiones Arithmeticae" die folgende Notation ein: $a \equiv b \bmod. c$, wo a, b und c ganze Zahlen bedeuten, um auszudrücken, daß $a - b$ durch c ohne Rest teilbar sei. Auch wenn a und b ganzzahlige Formen von Unbestimmten $x_1, \cdots, x_m$ bedeuten, benutzte Gauß die obige Schreibweise, sobald jeder Koeffizient von $a - b$ durch c ohne Rest teilbar war. Gauß und nach ihm Schönemann, Galois und neuerdings Hensel zeigten in Untersuchungen, welche sich auf alle Teile der Algebra und algebraischen Funktionentheorie beziehen, daß das Zeichen $\equiv$, wie es oben definiert war, viele, und wenn c eine Primzahl ist, alle algebraischen Eigenschaften des Gleichheitszeichens $=$ hat. Von den tiefsinnigen Untersuchungen von Galois und denen von Hensel können und wollen wir hier absehen, doch sind die Ideenbildungen von Schönemann, wie er sie in Crelles Journal veröffentlichte, für unseren Zweck von Bedeutung. Wenn c eine Primzahl ist und zwei modulo c kongruente Zahlen oder Formen als identisch angesehen werden, so gelten für die Gesamtheit aller modulo c inkongruenten Zahlen und Formen das assoziative und distributive Gesetz der Addition und Multiplikation, ferner gilt

$$a_1(a_2 + a_3) \equiv a_1 a_2 + a_1 a_3,$$

sowie die Eigenschaft der Null, nur dann einem Produkt gleich sein zu können, wenn einer der Faktoren ihr gleich ist. Da nun die Algebra nur auf den angeführten Gesetzen basiert, so kann man, ohne Irrtümer zu begehen, in einer Kette irgendwelcher algebraischen Identitäten oder Operationen das Zeichen $=$ überall durch $\equiv$ mod. c ersetzen.

Diesen wichtigen Grundsatz wollen wir das Prinzip von Schönemann nennen.

Das Wort „Ideal", wiewohl noch nicht der Begriff, wie er hier bestimmt ist, entstammt den schönen Untersuchungen von Kummer über algebraische Zahlen. Zu der Zeit, als Dirichlet, Eisenstein und Kummer an der Berliner Universität gemeinsam wirkten, entstanden viele der Untersuchungen, die in Dedekinds Ausgabe von Dirichlets Zahlentheorie durchgeführt sind. Danach werden Zahlen, welche einer ganzzahligen Gleichung

$$x^n + c_1 x^{n-1} + \cdots + c_n = 0$$

genügen, ganze algebraische Zahlen genannt, und, wenn α einer irreduziblen Gleichung n^{ten} Grades genügt, alle Zahlen der Gestalt

$$a_0 + a_1 \alpha + \cdots + a_{n-1} \alpha^{n-1},$$

wo die a_i rational, zum *Körper* (α) zusammengefaßt. Die verschiedenen Wurzeln einer und derselben irreduziblen Gleichung nennt man „konjugierte" Zahlen, das Produkt einer Zahl w mit ihren konjugierten die Norm derselben $N(w)$. Dirichlets Untersuchungen über die Einheiten eines gegebenen Körpers (α), d. h. diejenigen ganzen algebraischen Zahlen von (α), deren Norm $= \pm 1$ ist, sind klassisch geworden und gehören mit zu den schönsten der ganzen Mathematik. Kummer versuchte Jahre hindurch, die Teilbarkeitsgesetze der gewöhnlichen ganzen Zahlen auf diejenigen eines Körpers auszudehnen, doch lange Zeit ohne Erfolg, bis ihm die Lösung des Problems schließlich mit Hilfe der Konzeption der Idealzahlen gelang. Sind w_1, w_2 und $\frac{w_1}{w_2}$ *ganze* Zahlen des Körpers (α), so nennt er w_1 teilbar durch w_2. Ist sowohl $\frac{w_1}{w_2}$ wie $\frac{w_2}{w_1}$ ganz, so sind w_1 und w_2 für die Teilbarkeitsgesetze äquivalent. Da dann sowohl $N\left(\frac{w_1}{w_2}\right)$ wie $N\left(\frac{w_2}{w_1}\right)$ eine ganze Zahl, so muß $N(w_1) = \pm N(w_2)$, $\frac{w_1}{w_2}$ also eine Einheit sein. Eine ganze Zahl des Körpers (α), die nur durch sich selbst oder die Einheiten teilbar ist, könnte man eine Primzahl von (α) nennen, doch fand Kummer, daß ein Produkt von solchen Primgrößen sehr wohl durch andere solche Primgrößen teibar sein könne, die wesentliche Bedeutung der Primzahl bei diesen Primgrößen also verloren ging. Darum erfand er die *„Primideale"*.

Wenn eine Gleichung existiert

$$\beta_1\beta_2\cdots = \gamma_1\gamma_2\cdots,$$

wo die β_i und γ_i verschiedene Primgrößen in (α), so nahm Kummer Idealzahlen $(\beta_1, \gamma_1\gamma_2\cdots)$ und $(\beta_2, \gamma_1\gamma_2\cdots)$ an, welche sowohl β_1 wie $\gamma_1\gamma_2\cdots$ resp. β_2 wie $\gamma_1\gamma_2\cdots$ teilen. Die Idealzahl (β, γ) teilt jede Zahl $u\beta + v\gamma$, wo u, v ganze Zahlen von (α), und nur diese. Das Ideal (β, γ) teilt (δ, ε), wenn jede durch (δ, ε) teilbare Zahl durch (β, γ) teilbar ist. Ein Ideal, welches eine Einheit teilt, wird ausgeschieden, oder selbst Einheit. Ein Primideal ist ein solches, welches nur durch sich oder Einheiten teilbar ist. Alsdann ist in (α) jede ganze Zahl, wie auch jede Idealzahl, abgesehen von Einheiten als Produkt von Primidealen eindeutig bestimmt. Dies ist im Kern die Theorie von Kummer.

Ein interessanter Hilfsbegriff in Kummers Theorie ist der der „Äquivalenz" von Idealen. Danach sind zwei Ideale (β, γ), (δ, ε) äquivalent, wenn zwei ganze Zahlen λ, μ in (α) existieren, derart, daß

$$(\lambda\beta, \lambda\gamma) = (\mu\delta, \mu\varepsilon),$$

d. h. daß die Gesamtheit der Zahlen

$$\lambda\beta u + \lambda\gamma v$$

identisch ist mit der Gesamtheit der Zahlen

$$\mu\delta u + \mu\varepsilon v,$$

unter u, v beliebige ganze Zahlen in (α) verstanden.

Äquivalente Ideale faßte Kummer in einer „Idealklasse" zusammen und nannte diejenige Klasse, der die Einheit angehört, die Hauptklasse. Es stellte sich heraus, daß in jedem Körper (α) die Anzahl der verschiedenen Klassen endlich sei.

13. Die Kummersche Theorie wurde von Dedekind in folgerichtiger Weise nach jeder Richtung hin vervollkommnet. Der Begriff der Idealzahl, so wie ihn Kummer bestimmt hatte, schien noch etwas in der Luft zu schweben. Darum gab ihm Dedekind ein greifbares Substrat, indem er ein Ideal

$$(\beta, \gamma, \cdots, \lambda)$$

als die Gesamtheit der Zahlen der Gestalt

$$\beta u + \gamma v + \cdots + \lambda t$$

definierte, unter $u, v, \cdots$ ganze Zahlen verstanden, und nun an dieser Konzeption Kummers Ergebnisse nachwies. Er wandte dieselbe Methode auf die Theorie der algebraischen Funktionen und deren Integrale mit Erfolg an. Er führte den „Modul"-Begriff ein, indem er einen Modul $(\beta, \cdots, \lambda)$ als die Gesamtheit der Zahlen der Gestalt $\beta u + \gamma v + \cdots + \lambda t$

bestimmte, unter $u, v, \cdots, t$ rationale Zahlen verstanden. Er rechnete mit diesen Konzeptionen wie mit Zahlen, damit die Unabhängigkeit und Einheitlichkeit der eingeführten Begriffe drastisch vor Augen führend.

Dedekinds Zeitgenosse Kronecker realisierte den Kummerschen Idealbegriff auf ganz andere Weise. Die Idealzahl (β, γ) ersetzte er durch

$$N(\beta u + \gamma v) = k \cdot f(u, v),$$

unter $f(u, v)$ eine primitive homogene Form der Unbestimmten u, v, unter k eine ganze Zahl verstanden. Weber hat in einem neuerdings erschienenen Werke*) die Konsequenzen dieser Kroneckerschen Theorie gezogen. Auch J. König lehnt sich in seinem 1903 veröffentlichten ausgezeichneten Buche „Einleitung in die Theorie der algebraischen Größen" an die Ideen von Kronecker an. Der Modulbegriff erscheint bei Kronecker in der Gestalt von „Divisoren-Systemen". Um auszudrücken, daß eine Form F in der Gestalt

$$p_1 u_1 + p_2 u_2 + \cdots + p_h u_h$$

darstellbar sei, benutzt Kronecker die Schreibweise

$$F \equiv 0 \text{ mod.}(u_1, u_2, \cdots, u_h).$$

Dabei sind die u_i, p_i und F Polynome von Variablen und Unbestimmten in einem vorgegebenen „Rationalitätsbereiche" oder „Gattungsbereiche" (s. Festschrift zu Kummers Doktorjubiläum, Crelles Journal 92).

Die Begründung der Kummer-Dedekindschen Idealtheorie wurde neuerdings von Hurwitz in einfacher Weise erledigt. In seiner Abhandlung „Über die Theorie der Ideale", Gött. Nachrichten 1894, verfährt er wie folgt. In einem Körper K seien $\alpha, \cdots, \lambda$ bestimmte Zahlen, dann ist das Ideal

$$J = (\alpha, \cdots, \lambda),$$

die Gesamtheit der Zahlen

$$\alpha u + \cdots + \lambda t.$$

Ein „Hauptideal" besteht aus den Multipla einer einzigen ganzen Zahl von K. Ein Ideal J „teilt" ein anderes, J', wenn es alle Zahlen von J' enthält. Die Gesamtheit der ganzen Zahlen des Körpers K ist selbst als Ideal darstellbar, denn es läßt sich zeigen, daß es möglich ist, ganze Zahlen $\omega_1, \cdots, \omega_j$ in K zu finden, so daß jede ganze Zahl in K darstellbar ist in der Gestalt

$$\omega_1 u_1 + \cdots + \omega_j u_j,$$

unter $u_1, \cdots, u_j$ ganze rationale Zahlen verstanden. Das Ideal $(\omega_1, \cdots, \omega_j)$ heißt die „Einheit", und wird mit 1 bezeichnet. Die Einheit teilt alle Ideale. Das „Produkt" zweier Ideale

*) Lehrbuch der Algebra, Bd. 2.

$$J = (\alpha, \cdots, \lambda),$$
$$J' = (\alpha', \cdots, \mu')$$

wird JJ' geschrieben und ist

$$= (\alpha\alpha', \cdots, \lambda\mu').$$

Dasselbe ist offenbar teilbar durch J wie durch J'. Nach diesen Definitionen beweist Hurwitz

1) daß jedes Ideal J durch Multiplikation mit einem andern passend gewählten J' zu einem Hauptideal (a) gemacht werden kann, wo a eine rationale ganze Zahl; 2) daß irgend eine gegebene ganze rationale Zahl a nur zu einer *endlichen* Zahl von Idealen von K gehört; 3) daß aus einer Idealgleichung

$$J_1 J_2 = J_1 J_3$$

folgt

$$J_2 = J_3.$$

Denn ist J_1 so gewählt, daß $J_1 J' = a$ eine ganze rationale Zahl, so ergibt sich durch Multiplikation mit $J' : aJ_2 = aJ_3$, und hier läßt sich jede Seite offenbar durch a dividieren; 4) daß, wenn H ein Teiler von J, ein Ideal L existiert, das der Beziehung genügt

$$J = HL.$$

Wir brauchen, um L so zu bestimmen, nur H' so zu wählen, daß $HH' = (a)$. Alsdann ist jede Zahl von JH' teilbar durch a, und durch Ausführung der Division kommt

$$JH' = a \cdot L = HL \cdot H'$$

und nach 3)

$$J = HL.$$

5) Ein Ideal hat nur eine endliche Zahl von Teilern. Denn wenn $JJ' = (a)$, so gehört a zu jedem Teiler von J, die also nach 2) nur in endlicher Zahl vorhanden sein können. Aus diesen Sätzen erschließt Hurwitz genau nach der Methode der Theorie der ganzen rationalen Zahlen die Eindeutigkeit der Zerlegung eines Ideals

$$J = (p_1^{n_1}, \cdots, p_j^{n_j})$$

in ein Produkt von „Primidealen". Der einzige einigermaßen verwickelte Nachweis der Sätze 1) bis 5) ist der des Satzes 1). Hurwitz erbringt ihn nach zwei Methoden (die zweite findet sich in den Göttinger Nachrichten Okt. 1895 veröffentlicht).

Von den Anwendungen der Kummerschen Idealtheorie seien hier diejenige von Kummer zum Beweise der Unmöglichkeit der ganzzahligen Auflösung der Beziehung $x^p + y^p = z^p$ (außer der trivialen $x = 0$, $y = z$) für eine unendliche Anzahl von Zahlen p, sowie diejenige von Hurwitz

über die Gruppe von linearen Substitutionen, deren Koeffizienten ganze Zahlen des Körpers K sind und deren Determinante $= 1$ ist, erwähnt.

14. Von weittragendster Bedeutung für die Entwicklung des Modulbegriffes waren die Schriften von Salmon, welche um das Jahr 1850 entstanden und außerordentlich reich waren an anregenden Gedanken. In seinen geometrisch-algebraischen Untersuchungen benutzte Salmon sehr häufig Formen der Gestalt:

$$au + bv + \cdots + cw,$$

wenn $u, v, \cdots, w$ gegebene, $a, b, \cdots, c$ unbestimmte Formen bezeichnen. Zu seiner Theorie der Raumkurven macht Cayley eine Bemerkung, welche einige Jahrzehnte später mit die Veranlassung gab zu dem schönen Theorem I von Hilbert. Es heißt dort, daß es möglich sein müsse, Formen $u, v, \cdots, w$, die eine vorgegebene Raumkurve enthalten, so auszuwählen, daß eine beliebige sie enthaltende Oberfläche F in der Gestalt

$$F = au + bv + \cdots + cw$$

ausdrückbar sein müsse. Salmon sowohl wie Cayley benutzen einen erst viel später, 1902, von Severi bewiesenen Satz, daß eine Form F, welche in den Punkten des „vollständigen Schnittes" eines Formensystems $u, v, \cdots, w$ (dessen Oskulante nicht verschwindet) verschwindet, darstellbar sein müsse durch $au + \cdots$. Diese Vermutung spielt besonders in den Untersuchungen über „the order of restricted systems of equations", in welchen viele merkwürdige Tatsachen zum erstenmal zum Vorschein kamen, eine große Rolle. Man hat Salmons Werk unterschätzt, weil seinen Methoden die Strenge der Beweisführung abging. Wie groß dieser Fehler auch sein mag, so darf man niemals die Bedeutung Salmons als des großen Problemstellers und Wegweisers vergessen.

15. Das Verdienst, die Mittelpunktstellung, welche die Methode der Modulsysteme in allen Fragen der Algebra einnimmt, klar und scharf erfaßt und erwiesen zu haben, gebührt M. Noether. In seinem „Fundamentaltheorem" schrieb er der weiteren Entwicklung die Bahnen vor, welche sie fortan wandeln mußte. Die einleitenden Worte, mit welchen Noether die Veröffentlichung seines Fundamentaltheorems in den Göttinger Nachrichten 1872 und den Math. Ann. Bd. 6 begleitete, sind noch heute von Interesse. Die Tendenz seiner Untersuchungen, so sagte er, sei, eine Lücke auszufüllen, welche in einer Reihe von Arbeiten über Geometrie und Funktionentheorie zu finden sei. Der Satz, daß die Gleichung einer ebenen algebraischen Kurve $f = 0$, welche das vollständige Schnittpunktsystem zweier anderer solcher Kurven $\varphi = 0$, $\psi = 0$ enthält, notwendig von der Gestalt

$$0 = f = A\varphi + B\psi,$$

unter A, B Polynome verstanden, sei, hört auf gültig zu sein, wenn das System von Werten, für welches $\varphi = 0, \psi = 0$, mehrfache Punkte enthält. Nichtsdestoweniger hat man von dem erweiterten Satze Gebrauch gemacht, ohne die notwendigen Voraussetzungen seiner Gültigkeit zu untersuchen. — Die von Noether konstatierte Lücke wurde durch Angabe seines Fundamentaltheorems vollständig ausgefüllt. Die notwendigen Beziehungen, welche eine um einen Schnittpunkt α, β von $\varphi = 0$ und $\psi = 0$ entwickelte Potenzreihe F

$$F = \sum_{0,0}^{\infty,\infty}{}_{n,m}\, c_{n,m}(x-\alpha)^n(y-\beta)^m$$

erfüllen muß, damit bis zu Termen beliebig hoher Ordnungen n, m Potenzreihen

$$a = \sum_{0,0}^{\infty,\infty}{}_{n,m}\, a_{n,m}(x-\alpha)^n(y-\beta)^m,$$

$$b = \sum_{0,0}^{\infty,\infty}{}_{n,m}\, b_{n,m}(x-\alpha)^n(y-\beta)^m$$

sich der Relation $F = a\varphi + b\psi$ gemäß finden lassen, mögen die „Koinzidenzrelationen" von (φ, ψ) im Punkte (α, β) genannt werden. Die notwendige und hinreichende Bedingung für ein Polynom f, in der Gestalt $f = A\varphi + B\psi$ darstellbar zu sein, wo A und B Polynome sind, beruht dann darin, daß f die Koinzidenzrelationen von (φ, ψ) in allen Schnittpunkten von $\varphi = 0$, $\psi = 0$ erfülle. Dies ist das Fundamentaltheorem. Dasselbe hat zu einer ausgedehnten Literatur Veranlassung gegeben. Voß, Stickelberger, Noether (1887), Bertini, Noether (1889 und 1892), Brill, Baker, Scott behandelten das Theorem in den Mathematischen Annalen, F. Severi bewies eine Ausdehnung des Theorems auf den vollständigen Schnitt einer Anzahl von Formen für einen speziellen Fall, wie bereits früher angegeben (in den „Rendiconti della R. Accademia dei Lincei", Rom 1902). J. König in seinem 1903 in deutscher Ausgabe, 1902 in ungarischer Sprache erschienenen Werke „Einleitung in die allgemeine Theorie der algebraischen Größen" bewies die Verallgemeinerung des Satzes auf m Polynome von m Variablen, die im Endlichen eine endliche Zahl von Schnittpunkten haben („Der verallgemeinerte Noethersche Satz" findet sich auf S. 389 des Buches). Eine ganze Reihe von Autoren untersuchten die zahlentheoretischen Analoga des Noetherschen Satzes, z. B. Hensel in Crelle 1897 und 1898 „Zurückführung der Divisorensysteme auf eine reduzierte Form", Hancock in Crelle 1898 und 1900 „Canonical forms for the representation of Kroneckers modular systems", „On the reduction of

Kronecker's modular systems whose elements are functions of two and three variables", Landsberg in Schriften, die in den Göttinger Nachrichten, wie auch der Encyklopädie der Math. Wissenschaften erschienen sind.

Nach einer andern Richtung ging Hilbert vor, der in einer 1893 in den Mathematischen Annalen veröffentlichten Arbeit nachwies, daß, wenn $F_1, \cdots, F_h$ beliebige Formen und F eine Form bedeutet, die in allen $F_1 = 0, \cdots, F_h = 0$ gemeinsamen Punkten verschwindet, eine Zahl k existieren muß, so daß

$$F^k = A_1 F_1 + \cdots + A_h F_h,$$

wo $A_1, \cdots, A_h$ Formen.

16. Die Anwendungen, welche Noether von seinem Satze machte in bezug auf die Theorie der Berührung von Kurven, die der algebraischen Funktionen einer Variablen (Brill-Noether), sowie die der Abelschen Integrale, hatten die Bedeutung des Modulbegriffes in ein helles Licht gerückt, aber es dauerte doch noch fast 20 Jahre, bis der nächste bedeutende Fortschritt sich vollzog. Derselbe ist D. Hilbert zu verdanken. Seine in den Math. Ann. Bd. 36, 1890, veröffentlichten Theoreme I—IV sind grundlegend für eine Theorie der Moduln. Die Theoreme haben den folgenden Inhalt.

Theorem I: Ist $F_1, \cdots, F_k, \cdots$ eine beliebig vorgegebene Folge von Formen, so läßt sich immer eine ganze Zahl h angeben, so daß für jeden Index $k > h$ Formen $p_1, \cdots, p_h$ existieren, welche die Beziehung $F_k = p_1 F_1 + \cdots + p_h F_h$ erfüllen.

Theorem II: Ist $F_1, \cdots, F_k, \cdots$ eine beliebig vorgegebene Folge ganzzahliger Formen, so läßt sich immer eine ganze Zahl h angeben, so daß für jeden Index $k > h$ ganzzahlige Formen $p_1, \cdots, p_h$ existieren, die die Beziehung $F_k = p_1 F_1 + \cdots + p_h F_h$ erfüllen.

Theorem III: Es seien $f_1, \cdots, f_h$ gegebene Formen.

Alle Lösungen der Gleichung

$$0 = X_1 f_1 + \cdots + X_h f_h$$

in Formen $X_1, \cdots, X_h$ sind dann darstellbar in der Gestalt

$$X_i = Y_1 A_{1,i} + Y_2 A_{2,i} + \cdots + Y_k A_{k,i},$$

wo $A_{j,i}$ für alle Indexpaare $j, i\,(j = 1, \cdots, k;\ i = 1, \cdots, h)$ berechenbare Formen, wo $Y_1, \cdots, Y_k$ beliebige Formen sind und wo die weitere Gleichung $X_i = 0$ keine Lösung $Y_1, \cdots, Y_k$ zuläßt, in der irgend eines der Y_i gleich 1 wäre.

Diese Gestalt der Lösungen sei „die erste Syzygie" von $(f_1, \cdots, f_h)$ genannt. Die Gleichungen $X_i = 0$ führen dann auf ein System von Lösungen $Y_i = Z_1 B_{1,i} + Z_2 B_{2,i} + \cdots + Z_l B_{l,i}$, in welchem die B und Z_i die den A und Y_i auferlegten Bedingungen analogen Beschränkungen erfahren. Dieses letztere System von Lösungen sei „die zweite Syzygie"

von $(f_1, \cdots, f_h)$ genannt. Wird die dritte, vierte, $\cdots$ Syzygie von $(f_1, \cdots, f_h)$ genau ebenso definiert, so bricht die Reihe derselben ab. Die Kette der Syzygien jedes Formensystems $(f_1, \cdots, f_h)$ ist endlich.

Theorem IV: Ist $f_1, \cdots, f_h$ die Basis eines Moduls, so ist die Anzahl der Bedingungen, die einer Form R^{ter} Ordnung auferlegt werden, wenn von ihr die Zugehörigkeit zum Modul $(f_1, \cdots, f_h)$ gefordert wird, eine Funktion von R, welche für genügend große Werte von R durch ein Polynom in R dargestellt wird.

17. Die Schriften, welche sich mit der Weiterentwicklung der Kummer-Dedekindschen Idealtheorie befassen, sind bereits zu zahlreich, als daß hier eine vollständige Liste derselben zu geben versucht werden könnte. *Übrigens sind die in dieser Theorie behandelten* Probleme wesentlich von den allgemeineren in dieser Schrift behandelten verschieden.

Von allem, was vorhergeht, benutzen wir für die nun folgende Deduktion nur die Definition, welche wir voraufgeschickt haben, und die im wesentlichen von Dedekind und Hilbert stammt, die Schreibweise von Gauß-Kronecker, das Prinzip von Schönemann und die Theoreme I und II von Hilbert. Der Beweis dieser Theoreme beruht auf einem Divisionsverfahren und auf einem Induktionsschlusse, ist somit ganz im Rahmen der elementaren Mittel zu erledigen, welche für unser Kapitel I in Anwendung kamen.

Theorem I schließt in sich ein, daß, wenn M irgend ein Modul ist, sich dann immer eine Anzahl Formen

$$u_1, u_2, \cdots, u_h$$

angeben lassen, so daß jede Form des Moduls M darstellbar ist in der Gestalt

$$p_1 u_1 + p_2 u_2 + \cdots + p_h u_h,$$

wo die $p_1, \cdots, p_h$ Formen sind. Denn man brauchte ja nur alle linearunabhängigen Formen R^{ter} Ordnung des Moduls M für alle sukzessiven Werte von R aufschreiben und dann das Theorem I auf diese Folge anzuwenden. Man kann daher jeden Modul als die Gesamtheit der Formen, die $\equiv 0$ nach einem gewissen Divisorensystem sind, auffassen, wie umgekehrt jede solche Gesamtheit von Formen auch einen Modul bildet. Um anzudeuten, daß eine Form F einem Modul M angehört, schreiben wir daher

$$F \equiv 0 \text{ mod. } M$$

und nennen ein System von Formen $u_1, \cdots, u_h$, welches für M die oben angegebene Eigenschaft erfüllt, ein Fundamentalsystem oder eine Basis von M.

Sind M und N zwei Moduln, so bilden die Gesamtheit der Formen, die sowohl M wie N angehören, wieder einen Modul. Denn gehören p und q M und N an, so gehört $ap + bq$ sowohl M wie N an, die Ge-

samtheit der Formen, welche sowohl M wie N angehören, hat daher die Eigenschaft, welche einen Modul definiert. Dieser durch M und N eindeutig bestimmte Modul wird von uns

$$[M, N]$$

geschrieben und „kleinstes Vielfaches" von M, N genannt werden.

Die Formen, welche als Summe zweier andern darstellbar sind, von denen die eine M, die andere N angehört, bilden einen Modul. Denn ist

$$p = p' + p'',$$
$$q = q' + q'',$$

wo

$$p' \equiv 0 \text{ mod. } M, \quad p'' \equiv 0 \text{ mod. } N,$$
$$q' \equiv 0 \text{ mod. } M, \quad q'' \equiv 0 \text{ mod. } N,$$

so ist

$$ap + bq = (ap' + bq') + (ap'' + bq''),$$

wo

$$ap' + bq' \equiv 0 \text{ mod. } M,$$
$$ap'' + bq'' \equiv 0 \text{ mod. } N,$$

$ap + bq$ genügt also auch der Forderung.

Dieser durch M und N eindeutig bestimmte Modul wird (M, N) geschrieben und „größter gemeinschaftlicher Teiler" von M und N genannt werden.

Sind $M_1, M_2, \cdots, M_k$ eine Anzahl von Moduln, so ist

$$[M_1, M_2, \cdots, M_k] = [[M_1, M_2, \cdots, M_{k-1}], M_k],$$
$$(M_1, M_2, \cdots, M_k) = ((M_1, M_2, \cdots, M_{k-1}), M_k).$$

Nach dieser Definition ist es klar, daß in bezug auf die Operation $[\cdots]$ wie $(\cdots)$ das assoziative wie distributive Gesetz Geltung hat.

Es sei $u_1, u_2, \cdots, u_h$ eine Basis von M. Die Formen, welche mit irgend einem der u_i multipliziert Formen ergeben, die N angehören, bilden einen Modul.

Denn ist

$$p \cdot u_1 \equiv 0 \text{ mod. } N, \quad q \cdot u_1 \equiv 0 \text{ mod. } N,$$
$$p \cdot u_2 \equiv 0 \text{ mod. } N, \quad q \cdot u_2 \equiv 0 \text{ mod. } N,$$
$$\cdots\cdot \qquad \cdots\cdot$$
$$p \cdot u_h \equiv 0 \text{ mod. } N, \quad q \cdot u_h \equiv 0 \text{ mod. } N,$$

so ist auch $(ap + bq)\mathrm{u}_i = 0$ mod. N für jeden Index i.

Der Modul, der soeben definiert ist, ist von der besonderen Auswahl der Basis $u_1, \cdots, u_h$ ganz unabhängig und hängt nur von M und N ab, die sie eindeutig bestimmen. Denn aus obigen Kongruenzen folgt, daß, wenn f dem eben definierten Modul angehört, und

$$F = p_1 u_1 + p_2 u_2 + \cdots + p_h u_h$$

irgend eine Form von M ist, dann immer

$$f \cdot F \equiv 0 \text{ mod. } N.$$

Der Modul solcher Formen f wird $\frac{N}{M}$ geschrieben und „Residualmodul" von M in bezug auf N genannt werden.

Die Formen R^{ter} Ordnung, welche einem Modul M angehören, bilden eine „Involution", denn mit F_1 und F_2 gehört immer $c_1 F_1 + c_2 F_2$ zu diesem Formenbereiche, wo c_1, c_2 unbestimte Konstante bedeuten. Die Mannigfaltigkeit dieser Involution wird

$$\varphi(R) - H(M)(R)$$

geschrieben werden, wo $\varphi(R)$ die in Kap. I statuierte Bedeutung hat. $H(M)(R)$ wird „die Hilbertsche Funktion von M" genannt werden. Die Eigenschaften, welche Hilbert von ihr bewiesen hat, setzen wir nicht als bekannt voraus, so daß wir von ihr vorläufig weiter nichts wissen, als daß für jeden Wert von R ist: $H(M)(R) \leqq \varphi(R)$.

Es ist immer

$$H[M, N](R) + H(M, N)(R) = HM(R) + HN(R).$$

Diese Beziehung stammt von Hilbert und wird von ihm wie folgt bewiesen. Es sei

$$u_1, \cdots, u_h \text{ eine Basis von } M,$$
$$v_1, \cdots, v_k \text{ eine solche von } N.$$

Alsdann ist $u_1, \cdots, u_h, v_1, \cdots, v_k$ eine Basis von (M, N), da jede Form f, die zu (M, N) gehört, sich als Summe zweier Formen, die zu M und N gehören, schreiben lassen muß. Die Mannigfaltigkeit der Involution von Formen der Ordnung R, die sich schreiben lassen:

$$p_1 u_1 + \cdots + p_h u_h + q_1 v_1 + \cdots + q_k v_k,$$

ist also einerseits $= \varphi(R) - H(M, N)(R)$, andererseits gleich der Mannigfaltigkeit der Involution von Formen, die sich

$$p_1 u_1 + \cdots + p_h u_h$$

schreiben lassen, vermehrt um die Mannigfaltigkeit der Formen, die sich

$$q_1 v_1 + \cdots + q_k v_k$$

schreiben lassen, und vermindert um die Anzahl der linear-dependenten Relationen zwischen Formen dieser beiden Involutionen, d. h. die Mannigfaltigkeit der Involution von Formen der Ordnung R, die sowohl $\equiv 0$ mod. M, wie $\equiv 0$ mod. N sind, also $[M, N]$ angehören.

Damit zeigt sich, daß

$$\varphi(R) - H(M, N)(R) = \varphi(R) - HM(R) + \varphi(R) - HN(R) - \{\varphi(R) - H[M, N](R)\},$$

was die Behauptung verifiziert.

Wir fügen den obigen Definitionen noch die weiteren zu:

Ein Modul M, welcher die Eigenschaft hat, daß aus einer Beziehung $p \cdot q \equiv 0 \bmod. M$, wo p, q Formen sind, notwendig folgt, daß entweder

$$p \equiv 0 \bmod. M$$

oder

$$q \equiv 0 \bmod. M,$$

heißt ein „Primmodul".

Z. B. bildet die Gesamtheit der Formen, die in einem gegebenen Punkte verschwinden, einen Primmodul.

Schließlich wollen wir eine Form p, die die Eigenschaft hat, daß aus

$$p \cdot f \equiv 0 \bmod. M$$

unbedingt folgt

$$f \equiv 0 \bmod. M,$$

„relativ prim in bezug auf M" nennen.

Ist P ein Primmodul, so ist jede Form entweder $\equiv 0 \bmod. P$ oder relativ prim zu P.

Der Residualmodul von (p), der Multipla einer Form p, in bezug auf den Modul (P) ist immer mit p identisch, wenn p nicht $\equiv 0 \bmod. P$.

18. Wir gehen nun zu einer Reihenfolge von Schlüssen über, ausgehend von

Satz VI. „Wenn die Formen eines Moduls M keinen gemeinsamen Nullpunkt haben, so ist für genügend große Werte von R

$$HM(R) = 0."$$

Um dies zu erweisen, wählen wir aus M irgend eine Form f_1 aus, dann eine zweite f_2, welche mit f_1 keinen gemeinsamen Teiler hat. Eine solche existiert, da ja nicht *alle* Formen von M einen gemeinsamen Teiler haben können, der Voraussetzung nach. Wir wählen dann eine dritte f_3, deren Resultante mit f_1 und f_2 nicht verschwindet. Auch solche muß es geben, da kein Teil des Schnittes von $f_1 = 0$, $f_2 = 0$ auf jeder der Formen von M liegen kann, der gemachten Voraussetzung nach. So fortfahrend erhalten wir schließlich m Formen $f_1, \cdots, f_m$, welche sämtlich M angehören und deren Resultante nicht verschwindet.

Nun gehört jede Form der Gestalt

$$p_1 f_1 + \cdots + p_m f_m$$

M an, nach Satz II und III also jede Form einer genügend hohen Ordnung überhaupt. Damit ist Satz VI evident.

19. Ist $f_1, f_2, \cdots, f_h$ eine Basis eines Moduls M, so verschwinden die Formen von M in den Punkten der Konfiguration und nur in diesen

$$f_1 = 0,\ f_2 = 0, \cdots.$$

Wenn die Formen von M Gebilde der Mannigfaltigkeit h, jedoch keines von höherer Mannigfaltigkeit als h enthalten, so sagen wir, der Modul M habe die Mannigfaltigkeit h.

Wir definieren nun den Hauptbegriff der Modultheorie. Es sei P ein Primmodul der Mannigfaltigkeit h und Q ein Modul von höchstens der Mannigfaltigkeit h, welcher die Eigenschaft hat, daß aus einer Beziehung

$$A \cdot X \equiv 0 \text{ mod. } Q,$$

in welcher A eine gegebene Form, die *nicht*

$$\equiv 0 \text{ mod. } P,$$

immer folgt

$$X \equiv 0 \text{ mod. } Q.$$

Alsdann wird Q „ein primärer Modul", P der dazu gehörige Primmodul genannt. Besteht P aus der Gesamtheit der Formen, die das irreduzible Gebilde C enthalten, so enthalten alle Formen von Q C oder Q besteht aus der Gesamtheit *aller* Formen. Denn sei F eine Form von Q, die C nicht enthält, f eine beliebige Form, so ist $F \cdot f \equiv 0$ mod. Q, also, da F C nicht enthalten soll, $f \equiv 0$ mod. Q.

Es zeigt sich daher, daß der primäre Modul Q entweder die Mannigfaltigkeit h oder 0 hat; denn es folgt leicht, z. B. aus dem am Schlusse von Nr. 15 erwähnten Hilbertschen Satze, daß zu jedem Primmodul P ein irreduzibeles Gebilde C gehört, so daß jede C enthaltende Form P angehört, und vice versa.

Es gilt nun der folgende Satz, der Fundamentalsatz der Modultheorie, den ich den Noether-Dedekindschen Satz nennen will.

Satz VII. „Jeder Modul M ist darstellbar in der Gestalt

$$M = [Q_1, Q_2, \cdots, Q_k, R],$$

wo $Q_1, Q_2, \cdots, Q_k$ primäre Moduln und R ein Modul, dessen Formen keinen gemeinsamen Nullpunkt besitzen."

Es sei M von der Mannigfaltigkeit h. Die irreduziblen Bildungen der Mannigfaltigkeit h, welche den Formen von M gemein sind, seien mit $C_1, C_2, \cdots, C_j$ bezeichnet. Wir definieren nun einen Modul M_{C_1} durch folgende Bestimmung. M_{C_1} besteht aus der Gesamtheit der Formen F, deren Residualmodul $\frac{M}{(F)}$ nicht C_1 als ein ihren Formen gemeinsames Gebilde enthalte. Die Formen F sind also dadurch charakterisierbar, daß eine Form Φ existiert, welche C_1 nicht enthält und für welche

$$F \cdot \Phi \equiv 0 \text{ mod. } M.$$

Daß die Formen F einen Modul bilden müssen, zeigt sich leicht folgendermaßen:

Wenn $F_1\Phi_1 \equiv 0 \bmod. M$ und Φ_1 nicht C_1 enthält, sowie $F_2\Phi_2 \equiv 0 \bmod. M$ und auch Φ_2 nicht C_1 enthält, so ist für beliebige Formen A_1, A_2

$$(A_1F_1 + A_2F_2)\Phi_1\Phi_2 \equiv 0 \bmod. M,$$

also genügt, da $\Phi_1\Phi_2$ ja C_1 nicht enthält, auch $A_1F_1 + A_2F_2$ der gestellten Forderung.

Man kann M_{C_1} etwa dadurch bilden, daß man in der Involution der Formen R^{ter} Ordnung, die M angehören, die zerfallenden Formen aufsucht, und die Teiler, welche C_1 nicht enthalten, fortfallen läßt. Den Residualmodul von M_{C_1} in bezug auf M bezeichnen wir mit M'_{C_1}. Derselbe umfaßt also alle Formen X, die der Beziehung genügen

$$F_iX \equiv 0 \bmod. M,$$

wenn F_i ein Basissystem von M_{C_1} durchläuft. Die Formen von M'_{C_1} enthalten C_1 nicht als gemeinsames Gebilde. Denn sei $F_1, \cdots, F_j$ eine Basis von M_{C_1} und seien $\Phi_1, \cdots, \Phi_j$ Formen, die C_1 nicht enthalten und derart, daß $F_i \cdot \Phi_i \equiv 0 \bmod. M$. Alsdann ist

$$F_i \cdot \Phi_1 \cdot \Phi_2 \cdots \Phi_j \equiv 0 \bmod. M$$

für jeden Index i, somit gehört $\Phi_1 \cdot \Phi_2 \cdots \Phi_j$ dem Modul M'_{C_1} an. $\Phi_1 \cdot \Phi_2 \cdots \Phi_j$ enthält aber C_1 nicht.

Die Formen von M gehören sowohl dem Modul M_{C_1}, wie demjenigen M'_{C_1} an, da sie der an die Formen von M_{C_1} wie M'_{C_1} beziehungsweise gestellten Forderung genügen.

Ist F eine Form, welche dem Modul

$$[M_{C_1}, M_{C_2}]$$

angehört, und Φ eine solche, die dem Modul

$$(M'_{C_1}, M'_{C_2})$$

angehört, so ist $F \cdot \Phi \equiv 0 \bmod. M$. Denn Φ läßt sich zerlegen in eine Summe

$$\Phi = \Phi_1 + \Phi_2,$$

wo

$$\Phi_1 \equiv 0 \bmod. M'_{C_1},$$
$$\Phi_2 \equiv 0 \bmod. M'_{C_2}$$

und F gehört sowohl M_{C_1} wie M_{C_2} an, daher ist $F \cdot \Phi_1 \equiv 0 \bmod. M$, $F \cdot \Phi_2 \equiv 0 \bmod. M$ und $F \cdot \Phi \equiv 0 \bmod. M$.

Ebenso ist, wenn F eine Form von $[M_{C_1}, \cdots, M_{C_j}]$ und Φ eine Form von $(M'_{C_1}, \cdots, M'_{C_j})$, $F \cdot \Phi \equiv 0 \bmod. M$.

Der Modul $(M'_{C_1}, \cdots, M'_{C_j})$ enthält weder C_1 noch $C_2 \cdots$ noch C_j als ein seinen Formen gemeinsames Gebilde, denn dieser Modul enthält z. B. irgend eine Form von M'_{C_1}, die C_1 nicht enthält.

Wir können nun zeigen, daß identisch

$$M = [M_{C_1}, \cdots, M_{C_j}, (M, \overset{\circ}{\Phi})],$$

wo Φ irgend eine Form von $(M'_{C_1}, M'_{C_2}, \cdots, M'_{C_j})$, die weder C_1 noch $C_2 \cdots$ noch C_j enthält. Jede Form von M gehört jedem der Moduln

$$M_{C_1}, \cdots, M_{C_j}, (M, \Phi)$$

an. Umgekehrt, gehört F jedem dieser Moduln an, so existiert, da F auch (M, Φ) angehört, eine Form f, für die

$$F \equiv f \cdot \Phi \text{ mod. } M.$$

Da nun F dem Modul M_{C_1} angehört, M_{C_1} aber ein Teiler von M ist, so ist auch

$$f \cdot \Phi \equiv 0 \text{ mod. } M_{C_1}.$$

Nun ist der Modul M_{C_1} ein *primärer* Modul in bezug auf den Primmodul, der aus der Gesamtheit der C_1 enthaltenden Formen besteht. Denn ist A irgend eine Form, die C_1 nicht enthält, und ist angesetzt

$$A \cdot X \equiv 0 \text{ mod. } M_{C_1},$$

so wird diese Beziehung nur befriedigt, wenn eine Form Φ existiert, die C_1 nicht enthält und für die

$$A \cdot X \cdot \Phi \equiv 0 \text{ mod. } M.$$

Da nun A nicht C_1 enthalten soll, so ist

$$X \equiv 0 \text{ mod. } M_{C_1}.$$

Die Mannigfaltigkeit des erwähnten Primmoduls ist h, die von M_{C_1}, eines Teilers von M, höchstens h. Also ist M_{C_1} primär. Mithin folgt aus der Beziehung

$$f \cdot \Phi \equiv 0 \text{ mod. } M_{C_1},$$

da Φ C_1 nicht enthält,

$$f \equiv 0 \text{ mod. } M_{C_1};$$

und genau so zeigt sich

$$f \equiv 0 \text{ mod. } M_{C_i}$$

für jeden Index $i = 1, 2, \cdots, j$. Nun gehörte aber Φ dem Modul

$$(M'_{C_1}, \cdots, M'_{C_j})$$

an, somit ist nach dem schon früher Bewiesenen

$$f \cdot \Phi \equiv 0 \text{ mod. } M,$$
$$F \equiv 0 \text{ mod. } M.$$

Daher gehört jede Form, welche

$$[M_{C_1}, M_{C_2}, \cdots, M_{C_j}, (M, \Phi)]$$

angehört, M an, und da auch das Umgekehrte der Fall ist, so ist in der Tat

$$M = [M_{C_1}, M_{C_2}, \cdots, M_{C_j}, (M, \Phi)].$$

Der Modul (M, Φ) ist von der Mannigfaltigkeit $h-1$. Da er alle Formen von M enthält, so können seine Formen nur $C_1, \cdots, C_j$ und Gebilde niederer Mannigfaltigkeit gemein haben, und da Φ in $C_1, \cdots, C_j$ nicht verschwindet, so ist klar, daß die gemeinsamen Gebilde der Formen von (M, Φ) nur die Schnittgebilde von $\Phi = 0$ mit $C_1, \cdots, C_j$ und Gebilde niederer Mannigfaltigkeit sein können. Auf (M, Φ) wenden wir dasselbe Zerlegungsprinzip an, wie wir es bereits auf M angewandt haben, und schließlich erhalten wir so eine Beziehung:

$$M = [Q_1, \cdots, Q_j, R],$$

durch welche M in der Tat dargestellt ist als kleinstes Vielfaches von primären Moduln, deren zugehöriger Primmodul aus den Formen besteht, die in irreduziblen Gebilden verschwinden, und einem Modul, dessen Formen keinen gemeinsamen Nullpunkt haben. Aus obiger Reihe scheiden wir noch die (bei unserem Verfahren immer vorhandenen) Teiler Q aus, die bereits in anderen Q der Reihe enthalten sind, und erhalten dann als Schlußresultat eine Darstellung von M, wie sie Satz VII behauptete.

20. Satz VIII. „Wenn u eine Form der Ordnung a und relativ prim zu M ist, so ist

$$H(M, u)(R) = \Delta_a HM(R),$$

für alle Werte von $R \geqq a - m + 1$. Ist aber u nicht relativ prim zu M, so ist

$$H(M, u)(R) > \Delta_a HM(R).“$$

Es sei

$$f = C_1 f_1 + C_2 f_2 + \cdots + C_j f_j$$

ein unbestimmtes Glied der Involution von Formen der Ordnung R, die M angehören. Die Involution $pu + f$, wo p eine Form der Ordnung $R - a$, hat einerseits die Mannigfaltigkeit $\varphi(R) - H(M, u)(R)$, andererseits, nach dem schon mehrfach benutzten Satze, die von pu, plus der von f, vermindert um die von Identitäten der Form $pu + f = 0$. Es ist also

$$\varphi(R) - H(M, u)(R) = \varphi(R-a) + \varphi(R) - HM(R) - x,$$

wenn x die Mannigfaltigkeit der Identitäten

$$pu + f = 0.$$

Diese Beziehung ist sicherlich erfüllt, wenn

$$p \equiv 0 \text{ mod. } M,$$

und, wenn u relativ prim zu M, *nur* unter dieser Bedingung. Mithin ist

$$x = \varphi(R-a) - HM(R-a);$$

denn dies ist die Mannigfaltigkeit von Formen p der Ordnung $R - a$, welche M angehören. Daraus folgt

$$H(M, u)(R) = \Delta_a HM(R).$$

Ist $R < a$, so ist $x = 0$, weswegen für die Gültigkeit der Formel sich die untere Grenze

$$R = a - m + 1$$

ergibt. Für kleinere Werte von R ist die Formel durch Einsetzen von $x = 0$ zu korrigieren.

Es zeigt sich noch, daß, wenn für eine bestimmte Ordnung R

$$H(M, u)(R) = \Delta_a HM(R),$$

dann aus einer Beziehung der Ordnung R

$$p \cdot u \equiv 0 \text{ mod. } M$$

unbedingt folgen muß

$$p \equiv 0 \text{ mod. } M.$$

21. Satz IX. „Die Hilbertsche Funktion eines Moduls ist für genügend große Werte von R gleich einem Polynom von R, dessen Grad um 1 kleiner ist als die Mannigfaltigkeit des Moduls."

Wir wissen bereits aus Satz VI, daß die Hilbertsche Funktion eines Moduls, dessen Formen keinen gemeinsamen Nullpunkt haben, für genügend große Werte von R Null ist. Sei nun ein Modul M vorgelegt, dessen Formen nur eine Anzahl Punkte gemein haben. Nach Satz VII können wir denselben als kleinstes Vielfache darstellen

$$M = [Q_1, Q_2, \cdots, Q_j, R],$$

wo die

$$Q_1, Q_2, \cdots, Q_j$$

in bezug auf je einen der gemeinsamen Punkte der Formen von M primär. Ist u irgend eine Form, die keinen dieser Punkte enthält, so ist u relativ prim in bezug auf $Q_1, \cdots, Q_j$. Aus der Beziehung

$$u \cdot X \equiv 0 \text{ mod. } M$$

folgt daher

$$X \equiv 0 \text{ mod. } Q_1,$$
$$X \equiv 0 \text{ mod. } Q_2 \text{ etc.}$$

Soll X von genügend hoher Ordnung sein, so ist auch

$$X \equiv 0 \text{ mod. } R,$$

also

$$X \equiv 0 \text{ mod. } [Q_1, \cdots, Q_j, R] \equiv 0 \text{ mod. } M;$$

u ist somit relativ prim zu M, wenigstens wenn R genügend groß, und nach Satz VIII ist dann

$$H(M, u)(R) = \Delta_a HM(R),$$

wenn a die Ordnung von u. Nun haben die Formen von (M, u) keinen gemeinsamen Punkt, somit ist für genügend großes R

$$H(M, u)(R) = 0.$$

Demnach ist für genügend große R

$$\Delta_a HM(R) \equiv 0.$$

Wählen wir a der Einfachheit halber $= 1$, so zeigt diese Differenzengleichung, daß für genügend große R

$$HM(R) = a,$$

wo a eine von R unabhängige ganze Zahl, die nicht 0 sein kann, da die Formen von M Punkte gemein haben, nicht jede Form also M angehören kann.

Es mögen nun die Formen von M Kurven und Punkte gemein haben. Wir stellen wieder M als kleinstes Vielfache nach Satz VII dar

$$M = [Q_1, \cdots, Q_j, R].$$

Ist u irgend eine Linearform, welche keines der Gebilde enthält, in bezug auf welche die Q_i primär sind, so ist genau wie früher zu zeigen, daß für genügend große R u relativ prim zu M ist. Somit ist nach Satz VIII für genügend große R

$$H(M, u)(R) = \Delta_1 HM(R).$$

Die Formen von (M, u) haben Punkte gemein, nämlich die Schnittpunkte der den Formen von M gemeinsamen Kurven mit $u = 0$, somit existiert eine von 0 verschiedene ganze Zahl a derart, daß

$$a = \Delta_1 HM(R).$$

Es ist daher $HM(R) = aR + b$, wo b eine positive oder negative ganze Zahl, die auch 0 sein kann. Durch genau dieselben Schlüsse wird nun der Satz IX allgemein bewiesen.

22. Satz X. „Ist M ein primärer Modul und ist der zugehörige Primmodul P die Gesamtheit der Formen, welche das irreduzible Gebilde C enthalten, so läßt sich eine positive ganze Zahl k bestimmen, die derart ist, daß die k^{te} Potenz irgend einer Form von P dem Modul M angehört."

Zum Beweise der Behauptung entwickeln wir zunächst einen Hilfssatz. Derselbe besagt, daß, wenn $M^{(1)}, M^{(2)}, \cdots$ eine unendliche Reihe von Moduln ist, sich immer eine Zahl n angeben läßt, so daß der Modul

$$(M^{(1)}, M^{(2)}, \cdots, M^{(n)})$$

jeden Modul $M^{(N)}$ teilt, wie groß auch N sei.

Bezeichnen wir nämlich eine Basis von $M^{(i)}$ mit

$$u_{i,1}, u_{i,2}, \cdots, u_{i,j_i}$$

und wenden wir Hilberts Theorem (I) (s. Nr. 16) auf die unendliche Reihe dieser Formen, von $i = 1$ bis $i = \infty$ an, so zeigt sich, daß man eine Zahl n bestimmen kann, derart, daß jede Form $u_{i,j}$, wo $i > n$, dem

Modul $(u_{1,1}, \cdots, u_{n,j_n})$ angehört. Für dieselbe Zahl n ist daher $(M^{(1)}, \cdots, M^{(n)})$ ein Teiler von $M^{(i)}$, wo $i > n$.

Ist insbesondere jedes der $M^{(i)}$ obiger Reihe ein Teiler von $M^{(i-1)}$, so ist die wie oben bestimmte Zahl n so beschaffen, daß $M^{(n)} = M^{(n+1)} =$ etc., denn $(M^{(1)}, M^{(2)}, \cdots, M^{(n)})$ ist $= M^{(n)}$, weil $M^{(n)}$ ein Teiler aller $M^{(i)}$, wo $i < n$. Da nach obigem Hilfssatze $(M^{(1)}, \cdots, M^{(n)})$ $M^{(i)}$ teilt, für $i > n$, so teilt $M^{(n)}$ jedes $M^{(i)}$, wo $i > n$. Andererseits teilt auch $M^{(i)}$ das $M^{(n)}$ für $i > n$, nach Voraussetzung. Also ist $M^{(i)} = M^{(n)}$, wenn $i > n$.

Sei nun $F_1, F_2, \cdots, F_h$ eine Basis von P. Wir bilden

$$F = p_1 F_1 + p_2 F_2 + \cdots + p_h F_h,$$

wo die $p_1, \cdots, p_h$ Formen irgend eines positiven Grades, der auch Null sein kann, deren Koeffizienten aber sämtlich in der nun folgenden Rechnung unbestimmt sein sollen. Alsdann bilden wir den Residualmodul $M' = \frac{M}{(F)}$, was trotz der Unbestimmtheit der Koeffizienten von F möglich ist, denn die Kongruenz

$$F \cdot X \equiv 0 \text{ mod. } M$$

verlangt zu ihrer Auflösung für jede gegebene Ordnung von X nur die Auflösung einer Reihe von linearen Gleichungen, und dies ist eine Operation, die auch mit Unbestimmten sich vollziehen läßt. Ebenso bilden wir den Modul $M'' = \frac{M'}{(F)}$, dann $M''' = \frac{M''}{(F)}$ und so fort. In dieser Reihe ist jeder Modul $M^{(i)}$ ein Teiler des vorhergehenden, somit muß eine Zahl k existieren, so daß $M^{(k)} = M^{(k+1)}$. Jeder der $M^{(i)}$ ist ein primärer Modul in bezug auf P. Beweisen wir dies z. B. von M'. Sei A eine Form, die nicht in P enthalten ist. Sei ferner angesetzt

$$A \cdot X \equiv 0 \text{ mod. } M'.$$

Alsdann ist

$$F \cdot A \cdot X \equiv 0 \text{ mod. } M,$$

somit, da M primär,

$$F \cdot X \equiv 0 \text{ mod. } M$$

und

$$X \equiv 0 \text{ mod. } M'.$$

Auch ist die Mannigfaltigkeit von M', da es M enthält, kleiner als oder gleich der von P. Somit ist M' primär. $M^{(k)}$ ist also ein in bezug auf P primärer Modul, dessen Residualmodul in bezug auf F mit sich selbst identisch ist. F ist also relativ prim zu $M^{(k)}$.

Wir haben schon früher (Nr. 19) gezeigt, daß die Formen eines in bezug auf P primären Moduls, welcher das Gebilde C nicht enthält, mit der Gesamtheit aller Formen identisch ist.

Da nun F relativ prim zu $M^{(k)}$, so kann $M^{(k)}$ nach Satz VIII und IX

C nicht enthalten. Somit ist $M^{(k)}$ mit der Gesamtheit aller Formen überhaupt identisch. Es ergibt sich also, gemäß der Definition von $M^{(k)}$

$$F \equiv 0 \text{ mod. } M^{(k-1)}$$

ebenso

$$F^2 \equiv 0 \text{ mod. } M^{(k-2)}$$

etc., bis sich zeigt

$$F^k \equiv 0 \text{ mod. } M.$$

Nun war

$$F = p_1 F_1 + \cdots + p_h F_h,$$

also

$$F^k = p_1^k F_1^k + k_1 p_1^{k-1} p_2 F_1^{k-1} F_2 + \cdots \equiv 0 \text{ mod. } M.$$

Auch waren die Koeffizienten der p sämtlich Unbestimmte. Durch die gewöhnlichen Methoden (Nullsetzen einiger der Unbestimmten, Anwendung der Substitution $u + u'$ für eine Unbestimmte u etc.) zeigt sich daraus

$$\begin{gathered} F_1^k \equiv 0 \text{ mod. } M, \\ F_1^{k-1} F_2 \equiv 0 \text{ mod. } M, \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ F_h^k \equiv 0 \text{ mod. } M. \end{gathered}$$

Somit ist auch $f^k \equiv 0$ mod. M, wo f irgend eine Form

$$f = q_1 F_1 + \cdots + q_h F_h$$

des Moduls P.

Als ein Korollar des Satzes X zeigt sich, daß die Formen eines in bezug auf P primären Moduls nur die Gebilde C gemein haben. Eine andere Folge des Satzes X ist der Satz von Hilbert:

Es sei f eine Form, die in allen den Formen $f_1, \cdots, f_h$ gemeinsamen Punkten verschwindet. Dann läßt sich immer eine Zahl n bestimmen, derart, daß

$$f^n \equiv 0 \text{ mod. } (f_1, f_2, \cdots, f_h).$$

Denn ist $(f_1, \cdots, f_h) = [Q_1, Q_2, \cdots, Q_j, R]$ nach Satz VII, so können die Gebilde, die zu den Q_i gehören, nur Punkte enthalten, welche gleichzeitig $f_1 = 0, \cdots, f_h = 0$ machen. f wird also jedes der zu den Q_i gehörigen Gebilde umfassen. Gehören nun zu $Q_1, \cdots, Q_j$ gemäß Satz X die Zahlen $k_1, \cdots, k_j$, so genügt es, n gleich der größten dieser Zahlen anzunehmen — wenn nur die Ordnung von f genügend groß ist —, um den Hilbertschen Satz zur Evidenz zu bringen. Nur dann, wenn die Ordnung von f nicht groß genug ist, muß man n größer wählen.

23. Satz XI. „Wenden wir Satz VII auf das Modulsystem

$$M = (u_1, u_2, \cdots, u_h)$$

an, wo $h \leqq m - 1$ und die Resultante von $u_1, \cdots, u_h$ mit $m - h$ Linearformen nicht identisch verschwindet. Es zeigt sich dann, daß identisch

$$M = [M_{C_1}, M_{C_2}, \cdots, M_{C_j}],$$

wo $C_1, C_2, \cdots, C_j$ die irreduziblen Gebilde, welche den Schnitt von $u_1 = 0, \cdots, u_h = 0$ ausmachen."

Nach Satz VII ist für jedes Modulsystem

$$M = [M_{C_1}, M_{C_2}, \cdots, M_{C_j}, N],$$

wo $C_1, C_2, \cdots, C_j$ die Gebilde höchster Mannigfaltigkeit, welche den Formen von M gemein sind, und wo N von niederer Mannigfaltigkeit als M ist. Sei nun eine solche Entwicklung auch für den Modul $M = (u_1, u_2, \cdots, u_h)$ angenommen und sei Φ irgend eine Form von N, welche keines der $C_1, \cdots, C_j$ enthält. Sei F eine Form des Moduls $[M_{C_1}, \cdots, M_{C_j}]$. Alsdann ist

$$F \cdot \Phi \equiv 0 \text{ mod. } \quad [M_{C_1}, \cdots, M_{C_j}, N] \equiv 0 \text{ mod. } M.$$

Nun verschwindet aber die Resultante von $\Phi, u_1, \cdots, u_h$ und $m - h - 1$ Linearformen nicht identisch, also ist nach Satz I (Kap. I) $F \equiv 0$ mod. M.

24. Genau dieselbe Reihe von Definitionen und Schlüssen, wie sie oben durchlaufen war, führt auch in bezug auf die Theorie der *ganzzahligen* Formen zu bedeutsamen Ergebnissen.

Die Formen, welche ein gegebenes irreduzibles ganzzahliges Gebilde enthalten, bilden ein Ideal, genauer ein Primideal, wenn wir als ein solches jedes Ideal J definieren, derart, daß $A \cdot B \equiv 0$ mod. J zu

$$A \equiv 0 \text{ mod. } J \quad \text{oder} \quad B \equiv 0 \text{ mod. } J$$

führt, unter A, B ganzzahlige Formen verstanden. Auch in der Algebra mod. p, wo p irgend eine Primzahl, gilt der Zerlegungssatz der Formen in irreduzible Teiler und gelten daher alle Erwägungen des Satzes IV, nach dem Prinzip von Schönemann. In dieser Algebra gibt es daher auch irreduzible Gebilde.

Sind $J_1, J_2, \cdots, J_k$ eine Anzahl von Idealen, so definiert $[J_1, J_2, \cdots, J_k]$ ein Ideal, das wir kleinstes Vielfaches von $J_1, \cdots, J_k$ nennen werden, und $(J_1, J_2, \cdots, J_k)$ ein anderes, das größter Teiler von $J_1, \cdots, J_k$ heißen wird. Die Definition dieser Ideale ist mit genau denselben Worten möglich, wie die der Moduln $[M_1, \cdots, M_k]$ und $[M_1, \cdots, M_k)$.

Ist G in der Algebra mod. p ein irreduzibles Gebilde, und ist J das Primideal, welches dem irreduziblen ganzzahligen Gebilde G entspricht, so ist (p, J) ein Primideal.

Denn ist angesetzt

$$A \cdot B \equiv 0 \text{ mod. } (p, J),$$

so ist

$$A \cdot B \equiv 0 \text{ mod. } J$$

in der Algebra mod. p, also, da G in dieser Algebra irreduzibel,

$$A \equiv 0 \text{ mod. } J$$

oder

$$B \equiv 0 \text{ mod. } J$$

in der Algebra mod. p, mithin A oder $B \equiv 0$ mod. (p, J).

Ist G ein mod. p irreduzibles ganzzahliges Gebilde der Mannigfaltigkeit h, J das entsprechende Primideal, und $J' = (p, J)$, so wollen wir das Primideal J' einen Primdivisor, p seine Grundzahl nennen und als seine Mannigfaltigkeit die Zahl $h - 1$ bezeichnen. J dagegen wollen wir einen ganzzahligen Primmodul nennen. Auf diese Weise zerteilen sich die Primideale in die beiden Klassen der Primdivisoren und ganzzahligen Primmoduln.

Es sei irgend ein Ideal A vorgelegt. Wir definieren seine Mannigfaltigkeit auf folgendem Wege: Nach dem Theorem II von Hilbert (Nr. 16) bleibt der Inhalt des Theorems I von Hilbert bestehen auch bei Beschränkung auf ganzzahlige Formen. Mithin hat jedes Ideal eine Basis ganzzahliger Formen, vorausgesetzt, daß man auch ganze Zahlen mit als Formen rechnet. Sei die Basis von A

$$F_1, F_2, \cdots, F_k.$$

Wir zerlegen irgend eine der F_i, z. B. F_1, in seine irreduziblen Teiler und spalten die Gruppe derselben in zwei Systeme S_1 und S_2. S_1 enthält diejenigen, welche auch $F_2, \cdots, F_k$ teilen.

Ist F' irgend ein Individuum von S_2, so bringen wir dasselbe zum „Schnitt" mit einem der F_i, sagen wir F_2, welche nicht durch F' teilbar sind. Wir bilden also die Resultante von

$$F', F_2, l_1, \cdots, l_{m-2},$$

unter $l_1, \cdots, l_{m-2}$ Linearformen mit unbestimmten Koeffizienten $y_{i,j}$ verstanden, und spalten sie als Form derselben in ihre irreduziblen Teiler. Diese Teiler bestehen aus zwei Gruppen, nämlich Primzahlen und wirklichen irreduziblen ganzzahligen Formen der $y_{i,j}$. Ist p eine Primzahl der ersten Gruppe, so verschwindet in der Algebra mod. p die Resultante von F' und F_2, mithin haben nach dem Prinzip von Schönemann beide Formen in jener Algebra einen gemeinsamen irreduziblen Teiler t und daher sind sowohl F', wie $F_2 \equiv 0$ mod. (p, t). Sind auch $F_3, F_4, \cdots, F_k \equiv 0$ mod. (p, t), so ist (p, t) ein den $F_1, F_2, \cdots, F_k$ gemeinsamer Primdivisor.

Wenn dies nicht der Fall, so bringen wir t in der Algebra mod. p mit einem der F_i zum Schnitt, welche nicht durch t mod. p teilbar sind, und verfahren weiterhin in der Algebra mod. p ganz nach der Vorschrift des Satzes IV. Ist andererseits G ein von den $y_{i,j}$ abhängiger irreduzibler Teiler der Resultante der $F', F_2, l_1, \cdots, l_{m-2}$, so entspricht ihm

ein ganzzahliger Primmodul P. Entweder ist nun $F_i \equiv 0$ mod. P für jeden Index i, oder dies ist nicht der Fall. In letzterem Falle bringen wir das P entsprechende Gebilde genau nach der Vorschrift des Satzes V zum Schnitt mit einem der F_i, das nicht $\equiv 0$ mod. P, und erhalten dabei wieder eine von Unbestimmten abhängige Form, die als irreduzible Teiler sowohl Primzahlen, wie irreduzible Formen zuläßt. In jedem Falle schreitet der Prozeß nach der Vorschrift des Satzes V vorwärts. Das schließliche Ergebnis ist, daß wir eine Reihe von Primdivisoren J und ganzzahligen Primmoduln P erhalten, derart, daß für jedes J und P der Reihe und für jeden Index i

$$F_i \equiv 0 \text{ mod. } J$$

und

$$F_i \equiv 0 \text{ mod. } P$$

und auch derart, daß irgend ein Punkt, der in der Algebra der ganzen Zahlen oder der Algebra mod. irgend einer Primzahl die $F_1, \cdots, F_k$ verschwinden macht, auf irgend einem der zu dem J oder P gehörigen Gebilde gelegen ist. Die Maximalmannigfaltigkeit der Ideale der Gruppe P, J nennen wir die Mannigfaltigkeit des Ideals A. Dabei ist es offenbar, daß sowohl die Gruppe der P, J wie jene Mannigfaltigkeit von der Auswahl der Basis von A unabhängig ist.

25. Satz XII. „Ist A ein Ideal, welches weder Primdivisoren noch ganzzahlige Primmoduln als Teiler zuläßt, so ist jede ganzzahlige Form F genügend hoher Ordnung $F \equiv 0$ mod. A."

Es sei $f_1, \cdots, f_k$ eine Basis von A. Wir setzen, der Methode von Kronecker folgend,

$$\begin{aligned} F_1 &= p_1 f_1 + \cdots + p_k f_k, \\ F_2 &= q_1 f_1 + \cdots + q_k f_k, \\ &\cdots\cdots\cdots \\ F_m &= r_1 f_1 + \cdots + r_k f_k, \end{aligned}$$

wo die $p_1, \cdots, p_k, \cdots, r_1, \cdots, r_k$ Formen mit lauter unbestimmten Koeffizienten, und bilden die Resultante von $F_1, \cdots, F_m$. Dieselbe kann weder in der Algebra der ganzen Zahlen, noch in derjenigen mod. irgend einer Primzahl identisch verschwinden, da sonst die $F_1, \cdots, F_m$, also auch $f_1, \cdots, f_k$, einen Primdivisor J oder ganzzahligen Primmodul t als Teiler zulassen müßten. Ist nun F von genügend hoher Ordnung und bezeichnen wir jene Resultante, die eine Form der Unbestimmten sein wird, mit Res, so besteht eine Identität:

$$\text{Res} \cdot F = A_1 \cdot F_1 + A_2 \cdot F_2 + \cdots + A_m \cdot F_m,$$

wo auch die $A_1, \cdots, A_m$ ganzzahlige Formen der Unbestimmten sein werden. Ordnen wir jede der Seiten obiger Identität nach den Potenz-

produkten der Unbestimmten und vergleichen wir die Koeffizienten der nämlichen Potenzprodukte, so ergibt sich eine Reihe von Kongruenzen

$$\begin{aligned} a_1 \cdot F &\equiv 0 \text{ mod. } (f_1, \cdots, f_k) \equiv 0 \text{ mod. } A, \\ a_2 \cdot F &\qquad\qquad\qquad\qquad \equiv 0 \text{ mod. } A, \\ &\cdots\cdots\cdots\cdots\cdots \end{aligned}$$

Die ganzen Zahlen $a_1, a_2, \cdots$ können keinen gemeinsamen ganzzahligen Teiler haben, da sie die Koeffizienten der Potenzprodukte der Unbestimmten in der Form Res sind und diese Form modulo keiner Primzahl verschwindet. Mithin existieren nach den Elementen der Zahlentheorie ganze Zahlen n_1, $n_2, \cdots$, so daß $n_1 a_1 + n_2 a_2 + \cdots = 1$, und es findet sich in der Tat

$$F \equiv 0 \text{ mod. } A.$$

26. Wir definieren nun ein primäres Ideal, in genauer Analogie mit der Definition des primären Moduls. Wenn aus

$$A \cdot B \equiv 0 \text{ mod } J,$$

wo J ein Ideal, A und B ganzzahlige Formen, von denen bekannt ist, daß

$$A \text{ nicht } \equiv 0 \text{ mod. } J',$$

wo J' ein Primideal, unbedingt folgt

$$B \equiv 0 \text{ mod. } J,$$

so ist J primär in bezug auf J', sobald die Mannigfaltigkeit von J' mindestens derjenigen von J gleich ist. Indem wir nun den Betrachtungen des Satzes VII dieses Kap. Wort für Wort folgen, erhalten wir

Satz XIII. „Jedes Ideal ist darstellbar als kleinstes Vielfache von primären Idealen und einem Ideale R, dessen Formen weder in der Algebra der ganzen Zahlen, noch in derjenigen modulo irgend einer Primzahl einen gemeinsamen Punkt haben."

27. Jedem Ideal entspricht ein Modul. Sind

$$u_1, u_2, \cdots, u_h$$

eine Serie ganzzahliger Formen, die eine Basis von J bilden, so definieren dieselben als Basis eines Moduls J' den J entsprechenden Modul. Dabei ist J' von der speziellen Auswahl der Basis $u_1, \cdots, u_h$ von J unabhängig, da ja jede Basis durch lineare Kombinationen einer andern ersetzbar ist. Gehört eine ganzzahlige Form f dem Modul J' an, so lassen sich Formen $p_1, \cdots, p_h$ bestimmen, derart, daß

$$f = p_1 u_1 + \cdots + p_h u_h.$$

Die Koeffizienten der p_i sind dabei aus einer Serie linearer Gleichungen, deren Koeffizienten ganze Zahlen sind, bestimmbar. Somit gibt es Formen p_ν, die obige Relation erfüllen, und deren Koeffizienten rationale Brüche sind. Zudem sind die Nenner dieser Brüche von den Koeffizienten von f unab-

hängig, wie bereits die elementare Theorie der Determinanten und linearen Gleichungen zeigt, wohl aber abhängig von der Ordnung R. Sei für eine bestimmte Ordnung R

$$g(R)$$

der Generalnenner der Brüche, welche die Koeffizienten von $p_1, \cdots, p_h$ bilden. Alsdann ist

$$g(R) \cdot f \equiv 0 \text{ mod. } J.$$

Alle ganzzahligen Formen von J' bilden ebenfalls ein Ideal, da mit zwei ganzzahligen Formen p, q, die J' angehören, auch $ap + bq$, wo a, b ganzzahlige Formen, eine ganzzahlige Form von J' ist. Sei dieses Ideal kurz $(\!(J')\!)$ geschrieben. Auch $(\!(J')\!)$ hat eine Basis

$$f_1, f_2, \cdots, f_k,$$

und da es ganze Zahlen gibt

$$g_1, g_2, \cdots, g_k,$$

so daß

$$g_i \cdot f_i \equiv 0 \text{ mod. } J,$$

so ist also, wenn

$$g = g_1 \cdot g_2 \cdots g_k$$

gesetzt wird

$$g \cdot f \equiv 0 \text{ mod. } J,$$

wo f irgend eine ganzzahlige Form von J'.

Wir definieren nun wie folgt:

Ein Primideal, welches eine ganze Zahl enthält, heiße ein Primdivisor.

Ein primäres Ideal, welches eine ganze Zahl enthält, heiße ein primärer Divisor.

Ein Produkt von primären Divisoren heiße ein Divisor.

Ein Primideal, welches kein Primdivisor ist, heiße ein ganzzahliger Primmodul.

Ein primäres Ideal, welches kein Divisor ist, heiße ein ganzzahliger primärer Modul.

Ein Produkt von ganzzahligen primären Moduln heiße ein ganzzahliger Modul.

Es zeigt sich dann: „Das zu einem primären Divisor gehörige Primideal ist ein Primdivisor.“ Denn genau wie früher für primäre Moduln bewiesen ist, kann gezeigt werden, daß jede Form eines primären Ideals zu seinem Primideal gehören muß. Wenn das primäre Ideal ein Divisor, so gehört ihm eine Zahl an, diese gehört also auch dem entsprechenden Primideal an, dasselbe ist also ein Divisor.

Umgekehrt gilt: „Ein zu einem Primdivisor d gehöriges primäres Ideal J ist ein Divisor.“ Zu d gehört eine Zahl, die wegen der funda-

mentalen Eigenschaft der Primideale eine Primzahl sein muß. Dieselbe sei p. Wir bilden nun die Reihe der Ideale

$$J,\ J_1 = \frac{J}{(p)},\ J_2 = \frac{J_1}{(p)},\ J_3 = \frac{J_2}{(p)}, \cdots, J_k = \frac{J_{k-1}}{(p)}, \cdots,$$

von denen jedes das vorhergehende teilt. Nach dem früher (Nr. 22) bewiesenen Satze muß es eine Zahl k geben, so daß

$$J_k = J_{k+1} = \cdots$$

J_k ist, wie nach dem schon früher angewandten Schlußverfahren gezeigt wird, ein primäres Ideal, dessen Primideal d ist. Bezeichnen wir J_k mit I, so ist

$$\frac{I}{(p)} = I.$$

Daraus ergibt sich aber

$$I = (\!(I')\!).$$

Denn ist f irgend eine Form von $(\!(I')\!)$, so gibt es eine Zahl g, so daß

$$g \cdot f \equiv 0 \text{ mod. } I.$$

Da aber g in Faktoren zerfällt, die entweder relativ prim zu d oder Potenzen von p sind — denn d enthält nur die Multipla der einen Primzahl p oder die Einheit, wie aus den Elementen der Zahlentheorie erweisbar —, andererseits $\frac{I}{(p)} = I$ war, so folgt

$$f \equiv 0 \text{ mod. } I,$$

d. h. in der Tat

$$I = (\!(I')\!).$$

Sei die Mannigfaltigkeit von d gleich h, so wird auch diejenige von J gleich h sein, und da alle Formen von J enthalten sind in $J_1, J_2, \cdots$, so wird die Mannigfaltigkeit von I höchstens $= h$.

Die Formen von I' werden eine Anzahl von Gebilden höchstens der Mannigfaltigkeit h gemeinsam haben, und diese Gebilde werden sich in Gruppen konjugierter Gebilde trennen lassen, nach Satz V. Sei f irgend eine ganzzahlige Form, welche jede Gruppe dieser konjugierten Gebilde enthält. Alsdann wird nach dem Satze X eine Zahl n existieren, so daß

$$f^n \equiv 0 \text{ mod. } I',$$

also, da f ganzzahlig,

$$f^n \equiv 0 \text{ mod. } (\!(I')\!),$$

$$f^n \equiv 0 \text{ mod. } I,$$

somit, da I primär in bezug auf d,

$$f \equiv 0 \text{ mod. } d,$$

wenn nicht I die Gesamtheit aller Formen bedeutet. Verweigern wir letztere Annahme, so müssen wir zugestehen, daß d Formen enthält, die

irreduzible Gebilde von höchstens der Mannigfaltigkeit h gemein haben. Außerdem enthält d noch p, müßte also von minderer als der Mannigfaltigkeit h sein und dies ist nicht der Fall. Somit muß zugestanden werden, daß I die Gesamtheit aller Formen ist. Daher enthält wegen der Identität $J_k = I$, J die Zahl p^k, J ist also ein Divisor.

Das Primideal, das zu einem primären ganzzahligen Modul gehört, ist also ein ganzzahliger Modul und vice versa.

Ist J irgend ein Ideal und seine Darstellung nach Satz XIII als Produkt von primären Idealen ausgeführt, so können wir nach obigem die primären ganzzahligen Moduln in eine Gruppe und die primären Divisoren in eine andere Gruppe zusammenfassen, so daß erhalten wird

$$J = [G, d, R],$$

wo G ein ganzzahliger Modul, d ein Divisor ist und R die frühere Bedeutung beibehalten hat.

G hat die durch $(\!(G')\!) = G$ ausgedrückte Eigenschaft. G läßt sich nämlich zerspalten in ein Produkt primärer ganzzahliger Moduln

$$G = [A, B, \cdots, C],$$

und es ist

$$(\!(G')\!) = [(\!(A')\!), (\!(B')\!), \cdots, (\!(C')\!)],$$

weil, wenn eine ganzzahlige Form $F(\!(A')\!), \cdots, (\!(C')\!)$ angehört, eine Zahl j existiert, so daß jF $[A, \cdots, C]$, also G angehört. Andererseits ist für primäre ganzzahlige Moduln $(\!(A')\!) = A$, denn das zu A gehörige Primideal ist nach früherem ein ganzzahliger Modul, aus einer Beziehung

$$g \cdot f \equiv 0 \text{ mod. } A$$

folgt daher

$$f \equiv 0 \text{ mod. } A.$$

Aus $J = [G, d, R]$ folgt

$$(\!(J')\!) = [(\!(G')\!) \cdot (\!(d')\!) \cdot (\!(R')\!)].$$

Nun gibt es eine Zahl g, welche d angehört, somit enthält (d') die Einheit und besteht aus der Gesamtheit aller Formen. Damit zeigt sich schließlich

$$(\!(J')\!) = [G_1 (\!(R')\!)].$$

Die Formen eines ganzzahligen Moduls sind also definiert durch ihre Zugehörigkeit zu einem Modul im ursprünglichen Sinn des Wortes und durch ihre Ganzzahligkeit. Die Formen eines Divisors haben aber ganz andere Eigentümlichkeiten. Es erübrigt noch, dieselben festzulegen.

28. Wir definieren, in Analogie mit den Festsetzungen der Zahlentheorie, ein *vollständiges Restsystem R^{ter} Ordnung des Divisors d* als eine Gruppe Γ von Formen, derart, daß jede beliebig ausgewählte ganzzahlige Form F einer Form der Gruppe Γ mod. d kongruent ist. Γ wird für jeden

Wert von R aus einer endlichen Anzahl von Formen bestehen, vorausgesetzt, daß nicht zwei Formen Γ angehören dürfen, die mod. d kongruent sind; denn selbst wenn die Basis von d nur aus der Zahl, die sie enthält, bestände, würde ja ein derartiges Restsystem eine endliche Zahl Glieder haben, und die anderen Glieder der Basis können die betreffende Anzahl nur verringern. Die Anzahl der Glieder von Γ sei als „Dedekindsche Funktion des Divisors d für die Ordnung R" bezeichnet und $Dd(R)$ geschrieben. Für sie gilt

Satz XIV: „Die Dedekindsche Funktion eines Divisors ist ein Produkt von Primzahlpotenzen

$$D\,d(R) = p_1^{a_1},\ p_2^{a_2}, \cdots, p_n^{a_n},$$

deren Basen von R unabhängig sind, und deren Exponenten von R abhängen, und zwar sind diese Exponenten für genügend große Werte von R Polynome von R. Dabei ist zum mindesten eines dieser Polynome vom Grade h, wenn die Mannigfaltigkeit von d gleich h ist, und keines ist von höherem Grade als h."

Wir erweisen den Satz durch Induktion. Er ist offenbar richtig, wenn die Resultante von m unbestimmten Formen von d eine primitive Form der Unbestimmten ist, denn dann gehört jede Form einer genügend hohen Ordnung d an. Hat d die Mannigfaltigkeit 0 (oder die Stufe m) und ist u irgend eine Form relativ prim zu den Primdivisoren der primären Teiler von d, mithin zu d, so haben die Formen von (d, u) kein Gebilde m^{ter} Stufe miteinander gemein und die Resultante von m seiner Formen mit unbestimmten Koeffizienten liefert eine primitive Form derselben. Jede beliebige Form F genügend hoher Ordnung genügt also einer Kongruenz

$$F \equiv qu \text{ mod. } d.$$

Ist $F_1, \cdots, F_j$ ein vollständiges Restsystem R^{ter} Ordnung von d, $q_1, \cdots, q_{k_i}$ ein solches der Ordnung $R-1$, u der Ordnung 1, so ist also

$$F_1 \equiv q_1 u \text{ mod. } d,$$
$$F_2 \equiv q_2 u \text{ mod. } d,$$
$$\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot$$

j ist $= i$. Denn einerseits ist keines der qu einem der anderen qu mod. d kongruent, weil ja aus

$$(q_i - q_j)u \equiv 0 \text{ mod. } d$$

folgen würde, da u relativ prim zu d,

$$q_i - q_j \equiv 0 \text{ mod. } d;$$

und diese Kongruenz widerspricht der Definition eines vollständigen Restsystems. Andrerseits kann nicht zu zwei mod. d inkongruenten Formen F dasselbe q gehören. Somit ist die Anzahl der Glieder eines vollständigen

Restsystems R^{ter} Ordnung von d für genügend hohe Werte von R konstant, wenn die Stufe von d gleich m ist.

Sei nun die Richtigkeit von Satz XIV angenommen, wenn die Stufe von d gleich k ist, und erschließen wir daraus seine Richtigkeit für die Stufenzahl $k-1$. Es sei wieder eine zu d relativ prime lineare Form u gewählt und das vollständige Restsystem R^{ter} Ordnung von (d, u) betrachtet.

Dasselbe sei $\Phi_1, \cdots, \Phi_b$. Das vollständige Restsystem R^{ter} Ordnung von d sei $F_1, \cdots, F_a$, das $(R-1)^{\text{ter}}$ Ordnung $q_1, \cdots, q_c$. Es ist dann für jeden Index i

$$F_i \equiv \Phi_j \bmod. (d, u)$$

oder

$$F_i \equiv \Phi_j + q_l u \bmod. d.$$

Der Definition von $\Phi_1, \cdots, \Phi_b$ nach ist für verschiedene Indizes i, i_1 $\Phi_i - \Phi_{i_1}$ immer inkongruent mod. (d, u). Eine Kongruenz

$$\Phi_j + q_l u \equiv \Phi_{j_1} + q_{l_1} u \bmod. d$$

führt also zu $j = j_1$ und

$$(q_l - q_{l_1}) u \equiv 0 \bmod d$$

d. h.

$$q_l \equiv q_{l_1}.$$

Somit ist die Anzahl a der F_i gleich der Anzahl aller Systeme von Φ_j und q_l, d. h. $= b \cdot c$. a ist aber $= Dd(R)$ und $c = Dd(R-1)$; b ist $= D(d,u)(R)$, also für genügend große R nach der gemachten Annahme, da ja (d, u) eine um 1 höhere Stufe als d hat, darstellbar in der Gestalt

$$p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n},$$

wo $p_1, \cdots, p_n$ verschiedene Primzahlen, $a_1, \cdots, a_n$ Polynome von R sind. Aus der Beziehung

$$\frac{Dd(R)}{Dd(R-1)} = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n}$$

folgt daher

$$Dd(R) = p_1^{A_1} \cdot p_2^{A_2} \cdots p_n^{A_n} \cdot c,$$

wo die $A_1, \cdots, A_n$ Polynome von R sind, deren Grad um 1 höher ist als der der entsprechenden Polynome $a_1, \cdots, a_n$, und wo c eine ganze von R unabhängige Zahl ist. Damit ist Satz XIV vollständig erwiesen.

29. Die Dedekindsche Funktion $Dd(R)$ eines Divisors d hat die Eigenschaft, daß eine mit ihr multiplizierte ganzzahlige Form F R^{ter} Ordnung dem Divisor d angehörte. Ist $u_1, \cdots, u_k$ eine Basis von d, F eine Form R^{ter} Ordnung mit lauter unbestimmten Koeffizienten y_i, sind $p_1, \cdots, p_k$ Formen mit lauter unbestimmten Koeffizienten z_i, und ist

$$F = p_1 u_1 + \cdots + p_k u_k,$$

so sind damit die y_i als ganzzahlige homogene lineare Funktionen der z_i definiert. Da d ein Divisor ist, so ist es möglich, wenn die y_i irgendwie gegeben sind, zugehörige z_i aus obigen Beziehungen zu berechnen. Beschränken wir aber die z_i auf ganzzahlige Werte, so werden die y_i nicht *beliebige* ganzzahlige Werte sein können, sondern sie werden gewissen Bedingungen genügen müssen. Ein Gesetz, welches in bezug auf derartige Beziehungen statt hat, ist von Stephen Smith und Frobenius entdeckt worden, und hat in seiner weiteren Ausgestaltung zu der fruchtbaren Theorie der „Elementarteiler" Anlaß gegeben. Dies Gesetz besagt folgendes: Sind $l_1, l_2, \cdots, l_n$ eine Reihe ganzzahliger linearer Formen von Unbestimmten z_i und ist die Zahl der Unbestimmten größer als n, so ist die Anzahl N der Systeme Γ ganzer Zahlen

$$(y_{1,1}, \cdots, y_{n,1}), (y_{1,2}, \cdots, y_{n,2}), \cdots, (y_{1,N}, \cdots, y_{n,N}),$$

von der Art, daß keines der Systeme von Gleichungen

$$y_{1,i} - y_{1,j} = l_1,\ y_{2,i} - y_{2,j} = l_2, \cdots, y_{n,i} - y_{n,j} = l_n$$

für verschiedene Indizes i, j eine Lösung besitzt, wohl aber jedes System

$$a_1 - y_{1,h} = l_1,\ a_2 - y_{2,h} = l_2, \cdots,$$

wo $a_1, \cdots, a_n$ beliebig gegebene ganze Zahlen, für einen der N Indizes $h = 1 \cdots N$ — diese Zahl ist genau gleich dem größten gemeinsamen Teiler der Determinanten der von den Koeffizienten der l_i gebildeten Matrix. — Die Unterdeterminanten jener Matrix haben eine Serie gemeinsamer Teiler, deren Verhältnisse die „Elementarteiler" bestimmen. Man kann alle betreffenden Sätze wohl am besten an der Hand der „Normalform" studieren, die Frobenius für das System der $l_1, \cdots, l_n$ aufstellt. Er ersetzt einerseits die z_i durch ein System von n ganzzahlig linear mit ihnen verbundenen Variablen z_i', derart, daß der größte gemeinsame Teiler aller Transformationsdeterminanten 1 ist; und andrerseits führt er denselben Prozeß auf die $l_1, \cdots, l_n$ aus, danach erhält er die transformierten l_i, die wir l_i' schreiben wollen, ausgedrückt in den z_i' in dieser Weise

$$l_1' = e_1 z_1',\ l_2' = e_1 e_2 z_2',\ l_3' = e_1 e_2 e_3 z_3', \cdots, l_n' = e_1 e_2 \cdots e_n z_n',$$

wo $e_1, \cdots, e_n$ ganze Zahlen sind. Für den Beweis dieses Satzes sei die klassische Abhandlung von Frobenius in Crelles Jounal 86 und 88 (Über lineare Formen) konsultiert.

Jedem beliebigen System von ganzzahligen Werten der z_i' und l_i' entsprechen infolge der Festsetzung über die Transformationsdeterminante ganzzahlige Werte der z_i und l_i, wie auch umgekehrt. Danach sind die Bedingungen, unter denen eine Serie von Gleichungen

$$l_1 = y_1,\ l_2 = y_2, \cdots, l_n = y_n$$

ganzzahlige Lösungen hat, genau angegeben durch

$$l_1' \equiv 0 \text{ mod. } e_1, \quad l_2' \equiv 0 \text{ mod. } e_1 e_2, \quad l_n' \equiv 0 \text{ mod. } e_1 e_2 \cdots e_n,$$

wo die l_i' gewisse ganzzahlig umkehrbare lineare Formen der l_i sind. Ist $a_1, \cdots, a_n$ ein System unbestimmter ganzer Zahlen, so ist $e_1 \cdots e_n = g$ die kleinste ganze Zahl, für die das Gleichungssystem $l_i = g \cdot a_i$ eine ganzzahlige Lösung hat. $e_1^n e_2^{n-1} \cdots e_n$ ist die früher N genannte Zahl.

Übertragen wir die Sätze von Frobenius auf die durch die Gleichung

$$F = p_1 u_1 + \cdots + p_h u_h$$

vermittelte Beziehung zwischen den y_i und z_i, so zeigt sich, daß für die Zahlen e_i des Systems dieser linearen Formen der z_i die Beziehung gilt

$$e_1 e_2 \cdots e_n = g(R),$$

wo $g(R)$ die kleinste ganze Zahl, für welche bei beliebiger ganzzahliger Form R^{ter} Ordnung F

$$g(R) \cdot F \equiv 0 \text{ mod. } d.$$

Ferner ist

$$e_1^n e_2^{n-1} \cdots e_n = D d(R).$$

Ist d ein Primdivisor, p die in d enthaltene Primzahl, so ist $g(R) = p$. Mithin ist nur *einer* der d entsprechenden Elementarteiler $= p$, die übrigen sind sämtlich $= 1$. $Dd(R)$ ist eine Potenz von p, deren Exponent für genügend hohe Werte von R, nach Satz XIV, ein Polynom ist. Dieser Exponent gibt nach der zweiten der obigen Beziehungen den Index des Elementarteilers an, der $= p$ ist. Ist d' ein primärer Divisor, so ist die kleinste ganze Zahl g, für die

$$g \cdot F \equiv 0 \text{ mod. } d',$$

wo F irgend eine Form, eine Potenz p^k einer Primzahl. Mithin ist aus

$$e_1 \cdots e_n = p^k$$

jeder der Elementarteiler eine Potenz von p und auch $Dd'(R)$ eine Potenz von p.

Man kann aus den Sätzen von Frobenius noch weitere Folgerungen ziehen. Ist d ein beliebiger Divisor, R eine bestimmte ganze Zahl, so lassen sich die Formen R^{ter} Ordnung von d in die Gestalt bringen

$$e_1 u_1 f_1 + e_1 e_2 u_2 f_2 + \cdots + e_1 \cdots e_n u_n f_n,$$

wenn $u_1, \cdots, u_n$ beliebige ganze Zahlen, $f_1, \cdots, f_n$ ein passend bestimmtes Fundamentalsystem aller ganzzahligen Formen R^{ter} Ordnung, $e_1, \cdots, e_n$ die wie oben durch die Elementarteiler bestimmten Zahlen sind. Obiges ist in der Tat nur eine Schreibweise der Normalform von Frobenius, für den vorliegenden Fall zur Anwendung gebracht. Nun ist $g = e_1 \cdots e_n$ die kleinste ganze Zahl, mit welcher multipliziert alle ganzzahligen Formen

R^{ter} Ordnung d angehören, und diese Zahl ist von R unabhängig. g ist bestimmbar als kleinste d angehörige Zahl. Aus der Beziehung $e_1 \cdots e_n = g$ geht hervor, daß nur eine endliche Zahl der e_i von 1 verschieden sind. Seien diese von 1 verschiedenen Zahlen e_i $E_1, E_2, \cdots, E_e$ genannt. Es ist dann

$$g = E_1 E_2 \cdots E_{e-1} E_e.$$

Die Indizes der von 1 verschiedenen e_i lassen sich dann immer, für genügend große Werte von R, als Polynome von R erweisen. Es ist nämlich die Darstellung der Formen R^{ter} Ordnung des Divisors, der aus allen Formen besteht, die mit $E_1 E_2 \cdots E_{e-1}$ multipliziert zu d gehören

$$u_1 f_1 + u_2 f_2 + \cdots + u_h f_h + E_e (u_{h+1} f_{h+1} + \cdots + u_n f_n),$$

denn diese und nur diese haben die angegebene Eigenschaft. Der Index E_e in diesem Divisor ist $h+1$, mithin ist

$$E_e^{n-h} = D\left(\frac{d}{E_1 \cdots E_{e-1}}\right)(R),$$

h also für genügend große Werte von R, nach Satz XIV, ein Polynom von R. Ebenso ist die Darstellung der Formen R^{ter} Ordnung des Divisors $\left(\frac{d}{E_1 \cdots E_{e-2}}\right)$

$$u_1 f_1 + \cdots + u_k f_k + E_{e-1}(u_{k+1} f_{k+1} + \cdots) + E_e E_{e-1}(U_{h+1} f_{h+1} + \cdots + U_n f_n).$$

Seine Dedekindsche Funktion ist

$$E_{e-1}^{2n-k-h} E_e^{n-k},$$

also ist auch der Index k von E_{e-1} ein Polynom von R. Und so kann man weiterschließen.

30. Satz XV. „Sind d_1, d_2 zwei beliebige Divisoren, so gilt für jeden Wert von R

$$D[d_1, d_2] \cdot D(d_1, d_2) = D d_1 \cdot D d_2."$$

Um dies zu erweisen, stellen wir vollständige Restsysteme R^{ter} Ordnung für d_1 und d_2 in folgender Weise her.

Sind A und B zwei Formen R^{ter} Ordnung dieses vollständigen Restsystems für d_1, so ist

$$A - B \text{ nicht } \equiv 0(d_1).$$

Sollen A und B auch zu einem vollständigen Restsystem für (d_1, d_2) gehören, so darf auch nicht $A - B \equiv 0(d_1, d_2)$ sein. Sicher wird es Formen geben, deren Differenz wohl zu (d_1, d_2), aber nicht zu (d_1) gehört. Sind A und B zwei solche Formen, so wird es möglich sein, $A - B$ als Summe $C + D$ zweier Formen herzustellen, von denen die erste d_1, die zweite d_2 angehört. B kann man nun in seinen Eigenschaften modulo d_1

durch $B' = B + C$ ersetzen, da $C \equiv 0 \bmod. d_1$. Tun wir dies, so wird, wegen $A - B = C + D$, $A - B' = D$ d_2 angehören.

Denken wir uns nun ein vollständiges Restsystem Γ von Formen R^{ter} Ordnung für d_1 hingeschrieben. Ist F irgend eine Form, so wird Γ eine Form A enthalten, von der Art, daß $F \equiv A \bmod. d_1$. Dann ist auch $F \equiv A \bmod. (d_1, d_2)$. Mithin werden die Formen von Γ mehr als genügen, ein Restsystem von (d_1, d_2) zu bilden. Greifen wir aus Γ diejenigen $a_1, \cdots, a_h$ heraus, welche ein vollständiges Restsystem von (d_1, d_2) bilden. Ist B irgend eine Form von Γ, die nicht gleich einem der a_i, so ist für irgend einen Index i

$$a_i - B \equiv 0 \bmod. (d_1, d_2),$$

denn sonst würden die a_i kein vollständiges Restsystem für (d_1, d_2) bilden. Ersetzen wir B durch $B' = B + C$ in der Weise, wie vorhin angegeben, so daß $a_i - B' \equiv 0 \bmod. d_2$ und $C \equiv 0 \bmod. d_1$, und nennen wir $(a_i - B')$ b_2, so ist $a_i + b_2$ ein Glied von Γ. Wenn dies für irgend einen Index i der Fall ist, so muß es auch der Fall sein für jeden Index i. $a_j + b_2$ kann nämlich nicht $\equiv a_i + b_2 \bmod. d_1$ sein, da a_j nicht $\equiv a_i \bmod. d_1$, und auch nicht $\equiv a_i$, da $a_j - a_i$ nicht $\equiv 0 \bmod. (d_1, d_2)$. Γ besteht somit zum mindesten aus den Formen a_i und $a_i + b_2$. Es sei B eine Form von Γ, die nicht unter den eben genannten enthalten ist. Alsdann verfahren wir genau wie oben und finden damit, daß B sich ersetzen läßt durch $a_i + b_3$, wo $b_3 \equiv 0 \bmod. d_1$ und i irgend ein bestimmter Index. Man kann nun wieder zeigen, daß $a_i + b_3$ für jeden Index i Γ angehören muß. Denn einerseits kann $a_i + b_3$ nicht $\equiv a_j + b_3 \bmod. d_1$ sein, weil a_i nicht $\equiv a_j$ $\bmod. d_1$, noch $a_i + b_3 \equiv a_j$ oder $a_j + b_2 \bmod. d_1$, da $a_i - a_j$ ja auch nicht $\equiv 0 \bmod. (d_1, d_2)$. So fortfahrend erschließen wir, daß Γ sich in die Gestalt bringen läßt

$$\begin{array}{l} a_1,\ a_1 + b_2,\ \cdots,\ a_1 + b_k \\ a_2,\ a_2 + b_2,\ \cdots,\ a_2 + b_k \\ \cdots \\ a_h,\ a_h + b_2,\ \cdots,\ a_h + b_k. \end{array}$$

Ebenso läßt sich das vollständige Restsystem von d_2 in die Gestalt bringen

$$\begin{array}{l} a_1,\ a_1 + c_2,\ \cdots,\ a_1 + c_l \\ a_2,\ a_2 + c_2,\ \cdots,\ a_2 + c_l \\ \cdots \\ a_h,\ a_h + c_2,\ \cdots,\ a_h + c_l, \end{array}$$

wo die c_i dem Modul d_1 angehören.

Ich behaupte nun, wenn noch der Kürze halber $b_1 = 0$, $c_1 = 0$ gesetzt wird, daß die $h \cdot k \cdot l$ Formen

$$a_i + b_j + c_n$$

ein vollständiges Restsystem für $[d_1, d_2]$ ausmachen.

Keine zwei dieser Formen sind mod. $[d_1, d_2]$ kongruent. Denn aus

$$a_i + b_j + c_n \equiv a_{i'} + b_{j'} + c_{n'} \text{ mod. } [d_1, d_2]$$

folgt

$$a_i \equiv a_{i'} \text{ mod. } (d_1, d_2),$$

also

$$i = i'$$

$$c_n \equiv c_{n'} \text{ mod. } (d_2),$$

also

$$a_i + c_n \equiv a_i + c_{n'} \text{ mod. } (d_1)$$

und

$$n = n',$$

ebenso

$$j = j'.$$

Ist F eine beliebige Form, so lassen sich Indizes i, j finden, derart, daß

$$F - a_i - b_j \equiv 0 \text{ mod. } d_1$$

und Indizes

$$i', n,$$

so daß

$$F - a_{i'} - c_n \equiv 0 \text{ mod. } d_2.$$

Dann ist

$$F - a_i - b_j - c_n \equiv 0 \text{ mod. } d_1$$

und

$$F - a_{i'} - b_j - c_n \equiv 0 \text{ mod. } d_2.$$

Durch Subtraktion kommt, wie leicht ersichtlich,

$$a_i - a_{i'} \equiv 0 \text{ mod. } (d_1, d_2),$$

somit $i = i' \cdot F - a_i - b_j - c_n$ gehört also sowohl d_1 wie d_2, d. h. $[d_1, d_2]$ an. F war aber eine beliebig zu wählende Form R^{ter} Ordnung.

Das System $a_i + b_j + c_n$ ist danach in der Tat ein vollständiges Restsystem R^{ter} Ordnung für $[d_1, d_2]$.

Nun ist

$$D[d_1, d_2] = hkl,$$

$$D(d_1, d_2) = h,$$

$$Dd_1 = hk,$$

$$Dd_2 = hl,$$

Satz XV infolgedessen evident. Es zeigt sich überdies, daß $D(d_1, d_2)$, Dd_1, Dd_2 Teiler sind von $D[d_1, d_2]$, und daß $D(d_1, d_2)$ ein Teiler ist von Dd_1.

31. Satz XVI. „Ist M ein ganzzahliger Modul, so lassen sich seine Formen R^{ter} Ordnung darstellen in der Gestalt

$$u_1 f_1 + \cdots + u_n f_n,$$

wo $u_1, \cdots, u_n$ beliebige ganze Zahlen und $f_1, \cdots, f_n$ geeignet ausgewählte ganzzahlige Formen sind. Dabei ist $n = \varphi(R) - HM(R)$, und es ist möglich, $h = HM(R)$ ganzzahlige Formen

$$f_{n+1}, \cdots, f_{n+h}$$

anzugeben, die mit $f_1, \cdots, f_n$ ein Fundamentalsystem aller ganzzahligen Formen R^{ter} Ordnung bilden."

Ist $F_1, \cdots, F_{n+h}$ irgend ein beliebiges Fundamentalsystem aller ganzzahligen Formen R^{ter} Ordnung, z. B. das System der Potenzprodukte der Variablen, so kann man die Form

$$F = v_1 F_1 + \cdots + v_{n+h} F_{n+h}$$

den h Bedingungen unterwerfen, M anzugehören, und so h lineare homogene ganzzahlige Gleichungen für die $v_1, \cdots, v_{n+h}$ herstellen. Seien dieselben etwa

$$l_1 = 0, \cdots, l_h = 0.$$

Haben die Determinanten der von $l_1, \cdots, l_h$ gebildeten Matrix einen gemeinsamen Teiler, und ist p ein Primzahlteiler desselben, so kann man in der Algebra modulo p nichtverschwindende Zahlen $w_1, \cdots, w_h$ bestimmen, derart, daß identisch $w_1 l_1 + \cdots + w_h l_h \equiv 0 \bmod. p$. Ist in dieser Beziehung w_1 eine von 0 verschiedene Zahl, so kann man das System

$$l_1, l_2, \cdots, l_h$$

ersetzen durch das andere

$$\frac{1}{p}(w_1 l_1 + \cdots + w_h l_h), \quad l_2, \cdots, l_h,$$

das auch ganzzahlig und dem ersteren äquivalent ist. Haben die Determinanten der von diesen Linearformen gebildeten Matrix noch einen gemeinsamen Teiler, so ist er jedenfalls kleiner als der des ersten Systems. So kann man fortfahren, bis schließlich ein System ganzzahliger Formen der v_i

$$L_{n+1}, \cdots, L_{h+h}$$

erhalten wird, die gleich 0 gesetzt, dieselben Bedingungen aussagen wie die Gleichungen $l_1 = 0, \cdots, l_h = 0$ und deren Matrix keinen gemeinsamen Teiler mehr enthält. Nun wählen wir irgend ein System ganzzahliger Linearformen der v_i: $L_1, \cdots, L_n$, so daß die Determinante der L_i gleich 1 ist. Dies ist nach den Elementen der Zahlentheorie möglich. Alsdann bestimmen sich die $f_1, \cdots, f_{n+h}$ aus der Identität

$$v_1 F_1 + \cdots + v_{n+h} F_{n+h} = L_1 f_1 + \cdots + L_{n+h} f_{n+h}$$

ebenfalls als Fundamentalsystem der Formen R^{ter} Ordnung, da ja die Transformationsdeterminante der $f_1, \cdots, f_{n+h}$ in bezug auf die $F_1, \cdots, F_{n+h}$ gleich 1 sein muß. Die Gestalt der letzteren Beziehung erweist die Behauptung.

32. Satz XVII. „Ist M ein ganzzahliger Modul der Stufe $m-1$ und f eine beliebig vorgegebene Form, so gibt es eine ganzzahlige Form F der Koeffizienten von f, deren Ordnung gleich der Hilbertschen Funktion von M ist und die nur verschwindet, wenn f nicht relativ prim zu M. Ist f relativ prim zu M, so ist (M, f) ein Divisor, und es gilt

$$D(M, f)(R) = F$$

für genügend große Werte von R."

Es sei h die Hilbertsche Funktion von M, k die Ordnung von F und R so groß gewählt, daß der Wert von $HM(R-k) = h$ ist. Stellen wir uns dann ein Fundamentalsystem der Ordnungen R und $R-k$ von M in der Weise her, wie es Satz XVI vorschreibt.

Die Funktionen $F_{n+1}, \cdots, F_{n+h}$ seien für die Ordnung R $a_1, \cdots, a_h$, für die Ordnung $R-k$ $b_1, \cdots, b_h$.

Die Formen R^{ter} Ordnung von (M, F) erscheinen in der Gestalt $u_1 f_1 + \cdots + u_n f_n + pf$, wo p eine ganzzahlige Form der Ordnung $R-k$. pf ist modulo M einer linearen Form der $a_1, \cdots, a_h$ kongruent

$$p \cdot f \equiv A_1 a_1 + \cdots + A_h a_h \text{ mod. } M,$$

wo die $A_1, \cdots, A_h$ von den Koeffizienten von p und f linear abhängen. p ist einer linearen Form der $b_1, \cdots, b_h$ kongruent

$$p \equiv B_1 b_1 + \cdots + B_h b_h \text{ mod. } M.$$

Die A_i sind also gewisse angebbare ganzzahlige lineare Formen der B_i. Nach den Sätzen von Frobenius-Smith enthält das vollständige Restsystem der Linearformen A_i, wenn die B_i irgendwelche ganzzahlige Werte annehmen, eine Anzahl Glieder, die durch den Wert der Determinante der A_i angegeben wird. Dieselbe ist eine ganzzahlige Form der Koeffizienten von f der Ordnung h und nur dann gleich 0, wenn die $A_1, \cdots, A_h$ linear-dependent sind, (M, f) also kein Divisor ist. Damit ist die Behauptung vollständig erwiesen.

Die Form F der Koeffizienten von f hat folgende Eigenschaften. Es ist identisch

$$F \cdot \Phi = p_1 u_1 + \cdots + p_h u_h + pf.$$

Hier bedeutet $u_1, \cdots, u_h$ eine Basis von M; $p, p_1, \cdots, p_h$ ganzzahlige Formen der $x_1, \cdots, x_m$ wie der Unbestimmten von f, Φ eine beliebig gegebene ganzzahlige Form, deren Ordnung genügend groß ist. Es ist dies eine unmittelbare Folge der Darstellbarkeit von F als Determinante. Die Form F ist primitiv. Wäre dies nicht der Fall, so würde F in der

Algebra modulo einer Primzahl p verschwinden, die $A_1, \cdots, A_h$ würden in dieser Algebra linear-dependent sein und die Formen von (M, f) hätten, was auch f sei, in der Algebra modulo p einen Punkt gemein. Die Formen von M hätten also in der Algebra modulo p Gebilde gemein, deren Stufe höchstens $m-2$ wäre, wären also teilbar durch Divisoren der Stufe $m-2$, was gegen die Voraussetzung verstößt, daß M ein ganzzahliger Modul der Stufe $m-1$ sein soll.

Es ist ferner

$$F(f) \cdot F(g) = F(f \cdot g),$$

d. h. das einem Produkte zweier Formen entsprechende F ist das Produkt der den beiden Formen beziehungsweise entsprechenden F. Setzen wir nämlich etwa

$$p \equiv z_1 \cdot d_1 + \cdots + z_h \cdot d_h \text{ mod. } M,$$

wo $d_1, \cdots, d_h$ die $f_1, \cdots, f_h$ der Ordnung von p, ferner in analoger Weise

$$\begin{aligned} p \cdot g &\equiv A_1 a_1 + \cdots + A_h \cdot a_h \text{ mod. } M \\ p \cdot f &\equiv B_1 b_1 + \cdots + B_h \cdot b_h \text{ mod. } M \\ p \cdot f \cdot g &\equiv C_1 c_1 + \cdots + C_h \cdot c_h \text{ mod. } M, \end{aligned}$$

so sind die $A_1, \cdots, A_h$ gewisse lineare Formen der Unbestimmten von g und der z_i, die $B_1, \cdots, B_h$ solche der Unbestimmten von f und der z_i, die $C_1, \cdots, C_h$ solche der Unbestimmten von f, g und der z_i. Nun ist die Determinante der letzteren in bezug auf die z_i teilbar durch die Determinante der $A_1, \cdots, A_h$ wie $B_1, \cdots, B_h$ in bezug auf die z_i, weil die $C_1, \cdots, C_h$ auch als ganze lineare Formen der $A_1, \cdots, A_h$ wie $B_1, \cdots, B_h$ darstellbar sind. Die Behauptung ist damit evident.

33. Eine andere Folge des Satzes XVI ist der folgende

Satz XVIII. „Ist M ein ganzzahliger Modul, n eine ganze Zahl, so ist

$$D(M, n)(R) = n^{HM(R)}."$$

Denn stellt man die Formen R^{ter} Ordnung in der Weise dar, wie es Satz XVI als möglich erweist, so zeigt sich, daß eine beliebige ganzzahlige Form mod. (M, n) einer Form der Gestalt

$$u_1 f_1 + \cdots + u_k f_k$$

kongruent ist, wo die u_i unabhängig voneinander die Werte $1, \cdots, n$ durchlaufen und $k = HM(R)$ ist. Diese Formen sind aber inkongruent mod. (M, n), die Behauptung also klar.

Es ist durch Satz XVIII die Möglichkeit gegeben, Sätze über Dedekindsche Funktionen sogleich in solche über Hilbertsche Funktionen ganzzahliger Moduln umzuwandeln.

34. Die Systeme von Formen

$$u_1, \cdots, u_h,$$

welche durch Primideale h^{ter} Stufe, aber nicht durch solche niederer Stufe teilbar sind, bilden Ideale, welche durch ebenso merkwürdige Eigenschaften ausgezeichnet sind wie die Moduln solcher Systeme. Es gilt.

Satz XIX. „Ist das Ideal

$$(u_1, \cdots, u_h)$$

nicht durch Primideale niederer als h^{ter} Stufe teilbar, und ist $h < m$, so ist identisch

$$(u_1, \cdots, u_h) = [Q_1, \cdots, Q_2, d_1, \cdots, d_j],$$

wo die Q_i und d_i primäre ganzzahlige Moduln und Divisoren h^{ter} Stufe sind.

„Ist $h = m$, so ist

$$(u_1, \cdots, u_h) = [d_1, \cdots, d_j, r],$$

wo $d_1, \cdots, d_j$ primäre Divisoren sind und r den Inbegriff der ganzzahligen Formen bedeutet, die apolar zu $\Omega(u_1, \cdots, u_m)$ oder von höherer Ordnung als Ω sind. Die Dedekindsche Funktion eines solchen Ideals $(u_1, \cdots, u_m)$ ist dem absoluten Werte der Resultante von $u_1, \cdots, u_m$ gleich und zwar für jeden Wert von R, der größer ist als $a_1 + \cdots + a_m - m$, wenn a_i die Ordnung von u_i bezeichnet."

Zunächst leiten wir einen Hilfssatz ab. Das Ideal $(u_1, \cdots, u_h)$ hat unendlich viele Basen, wenn $h > 1$. Zum Beispiel hat (u_1, u_2) die Basis $u_1, u_2 + pu$, wenn die Ordnung von u_2 größer als diejenige von u_1 oder ihr mindestens gleich ist und p irgend eine Form ist, deren Ordnung die Differenz der Ordnungen von u_1 und u_2. Wir werden nun zeigen, daß $(u_1, \cdots, u_h)$ eine Basis hat

$$v_1, v_2, \cdots, v_{h-1}, v_h$$

derart, daß

$$v_1, \cdots, v_{h-1}$$

die Basis eines ganzzahligen Moduls bilden.

Beweisen wir dies zunächst für $h = 2$. Ist eine der beiden Formen u_1, u_2 primitiv, so ist die Richtigkeit der Behauptung klar, denn man brauchte nur diese primitive Form $= v_1$ zu setzen, um die Forderung zu erfüllen. Sind beide imprimitiv und hat u_2 keine kleinere Ordnung als u_1, so muß unter den Voraussetzungen des Satzes XIX eine der Formen

$$u_2 + pu_1$$

primitiv sein. u_2 und u_1 können nämlich nicht beide durch dieselbe Primzahl teilbar sein, da sonst ihr Ideal die Stufe 1 hätte. Die gemeinsamen Teiler der Koeffizienten von u_2 und u_1 sind daher relativ prim zueinander,

Die Koeffizienten von $u_2 + pu_1$ sind somit lineare nicht homogene ganzzahlige Formen der Koeffizienten von p, und diese haben als Formen nicht einen gemeinsamen Teiler. Sie sind nicht für irgend ein Wertsystem der Koeffizienten von p Null. Man kann daher den letzteren solche Werte erteilen, daß die betreffenden Linearformen keinen gemeinsamen Teiler haben. Nachdem dies geschehen, ist $u_2 + pu_1$ eine primitive Form, die Basis

$$v_1 = u_2 + pu_1, \quad v_2 = u_1$$

erfüllt daher die Forderung des Hilfssatzes. Derselbe ist also bewiesen, wenn $h = 2$.

Beweisen wir den Hilfssatz durch Induktion. Sei die Richtigkeit des Satzes angenommen für den Wert $h - 1$. Ist u_h eine Form, deren Ordnung nicht größer ist als die einer der anderen u_i, so bestimmen wir Formen

$$v_1, \cdots, v_{h-2}, w,$$

deren Ideal dem von $u_1, \cdots, u_{h-1}$ äquivalent ist, und so, daß $v_1, \cdots, v_{h-2}$ einen ganzzahligen Modul bilden. Alsdann suchen wir p so zu bestimmen, daß $v_1, \cdots, v_{h-2}, w + pu_h$ einen ganzzahligen Modul bilden. Dies ist unter den Voraussetzungen des Satzes XIX immer möglich. $w + pu_h$ wird nicht eines der irreduziblen den $v_1, \cdots, v_{h-2}$ gemeinsamen Gebilde $C_1, \cdots, C_j$ enthalten. Bilden wir die Reihenfolge der Gleichungen, welche die Koeffizienten einer unbestimmten Form f derselben Ordnung wie w erfüllen müssen, damit sie eines der C_i enthalten, und ersetzen die Koeffizienten von f durch diejenigen von $w + pu_h$, so sind dieselben also durch kein Wertsystem der unbestimmten Koeffizienten von p identisch zu befriedigen, auch können sie keinen von den Unbestimmten unabhängigen gemeinsamen Teiler haben, da sonst modulo desselben das Ideal $u_1, \cdots, u_h$ die Stufe $h - 2$ hätte. Mithin kann man diesen Unbestimmten Werte erteilen, daß $w + pu_h$ modulo keiner Primzahl eines der $C_1, \cdots, C_h$ enthält. Dieses $w + pu_h$ setzen wir $= v_{h-1}$, $u_h = v_h$. Das Ideal $v_1, \cdots, v_{h-1}$ muß dann ein ganzzahliger Modul sein, da der Schnitt von $v_1, \cdots, v_{h-1}$ modulo jeder Primzahl relativ prim zu v_{h-1}. Der Hilfssatz ist somit erwiesen.

Sei zunächst $h = m$.

Wir ersetzen $u_1, \cdots, u_m$ durch ein ihm im Sinne des Hilfssatzes äquivalentes System $v_1, \cdots, v_m$, wobei $v_m = u_m$ die Form kleinster Ordnung des Systems. Da $v_1, \cdots, v_{m-1}$ ein ganzzahliger Modul, $v_1, \cdots, v_m$ ein Divisor, so ist die Dedekindsche Funktion des Ideals $(u_1, \cdots, u_m)$ gleich einer bestimmten primitiven Form F der Koeffizienten von u_m. Dabei ist die Ordnung von F gleich der Hilbertschen Funktion von $(v_1, \cdots, v_{m-1})$. Nun kann man aber nachweisen, daß die Dedekindsche Funktion eines Divisors von m Formen irgendwelcher Art

$$w_1, \cdots, w_m$$

für genügend große Werte von R immer durch die Resultante dieser Formen teilbar sein muß. Sind nämlich $w_1, \cdots, w_m$ Formen mit lauter unbestimmten Koeffizienten y_i, sind $a_1, \cdots, a_m$ die Ordnungen von $w_1, \cdots, w_m$, ist

$$R > a_1 + \cdots + a_m - m$$

und ist eine unbestimmte Form R^{ter} Ordnung f in der Gestalt

$$f = p_1 w_1 + \cdots + p_m w_m$$

angesetzt, wo die Koeffizienten der p_i Unbestimmte z_i, so können die z_i obiger Beziehung gemäß bei beliebig gegebenem f immer bestimmt werden, wenn $\operatorname{Res}(w_1, \cdots, w_m) \neq 0$, sonst aber nicht.

Daraus folgt dann, daß bei unbestimmten y_i die Determinanten $\varphi(R)^{\text{ter}}$ Ordnung des aus den Koeffizienten von $p_1 w_1 + \cdots + p_m w_m$, die ja Linearformen der z_i sind, gebildeten Systems teilbar sein müssen durch

$$\operatorname{Res}(w_1, \cdots, w_m).$$

Diese Determinanten haben daher für unbestimmte y_i, also erst recht für bestimmt gegebene Werte der y_i zum mindesten den gemeinsamen Teiler

$$\operatorname{Res}(w_1, \cdots, w_m).$$

$D(w_1, \cdots, w_m)(R)$ muß daher immer durch $\operatorname{Res}(w_1, \cdots, w_m)$ teilbar sein, wenn

$$R > a_1 + \cdots + a_m - m.$$

Bedeuten nun $a_1, \cdots, a_m$ die Ordnungen der $u_1, \cdots, u_m$ beziehungsweise $v_1, \cdots, v_m$, so folgt, daß für genügend große Werte von R die obengenannte Form F der Koeffizienten von u_m teilbar sein muß durch $\operatorname{Res}(v_1, \cdots, v_{m-1}, u_m)$. Aber die letztere ist von derselben Ordnung, nämlich $a_1 \cdots a_{m-1}$, wie F. Auch war F primitiv; also ist

$$F = \pm \operatorname{Res}(v_1, \cdots, v_{m-1}, u_m).$$

Man kann auch den Wert von R, von dem ab diese Gleichung gilt, ganz genau bestimmen. In der Ableitung von Satz XVII war der Wert von R so groß gewählt, daß der Wert von $HM(R-k) = h$ ist. Hierfür genügt es, im vorliegenden Falle nach Satz II $R > a_1 + \cdots + a_m - m$ zu wählen, denn dann ist die Gleichung

$$H(v_1, \cdots, v_{m-1})(R - a_m) = H(v_1, \cdots, v_{m-1})(R)$$

immer befriedigt. Die obige Gleichung gilt somit für alle Werte

$$R > a_1 + \cdots + a_m - m.$$

Dies beweist den letzten Teil des Satzes XIX.

35. Stellen wir nun $(u_1, \cdots, u_m)$ in der Weise des Satzes XIII dar

$$(u_1, \cdots, u_m) = [d_1, \cdots, d_j, r].$$

Wir werden dann zeigen, daß jede Form F R^{ter} Ordnung, wo

$$R > a_1 + \cdots + a_m - m,$$

welche zu $d_1, \cdots, d_j$ gehört, zum Ideal $(u_1, \cdots, u_m)$ gehören muß. Dies ist richtig, wenn $m = 2$ und eine der beiden Formen eine primitive Linearform ist. Denn dann ist (u_1, u_2) identisch mit $(R \cdot x^n, l)$, wo l die primitive Linearform, R die Resultante von u_1 mit l, x eine Variable, deren Determinante mit l die Einheit ergibt. Die primären Divisoren dieser Ideale sind daher von der Gestalt

$$p^h, l,$$

wo p die verschiedenen Primzahlen, welche in R aufgehen, durchläuft und p^h die höchste in R aufgehende Potenz von p ist. Also muß eine Form f, die all diesen primären Divisoren angehört und von der Ordnung n' ist, die Gestalt

$$R \cdot g + l \cdot g'$$

haben, wo g mod. l ein Multiplum von x^n ist. Wir erweisen die Behauptung allgemein durch Induktion, indem wir annehmen, daß die Behauptung zutreffe im Bereiche von $m - 1$ Variablen, wenn eine der Formen u_i primitiv und linear ist, und daraus herleiten, daß sie dann gilt im Bereiche von $m - 1$ Variablen überhaupt und im Bereiche von m Variablen, wenn eine der Formen primitiv und linear ist. Seien $w_1, \cdots, w_{m-2}, w_{m-1}$ $m - 1$ Formen im Bereiche von $m - 1$ Variablen, $w_1, \cdots, w_{m-2}$ bereits so ausgewählt, daß $(w_1, \cdots, w_{m-2})$ ein ganzzahliger Modul. Es sei l eine primitive und lineare Form, die zu $w_1, \cdots, w_{m-1}$ relativ prim ist. f sei eine Form der Ordnung R

$$R > a_1 + \cdots + a_{m-1} - m + 1,$$

wo a_i die Ordnung von w_i bezeichnet, und gehöre zu den primären Divisoren von $(w_1, \cdots, w_m)$.

Es wird nun nach Satz XIII eine Zahl R geben, so groß, daß f dann eo ipso zum Ideal $(w_1, \cdots, w_{m-1})$ gehört. Um nachzuweisen, daß diese Zahl $= a_1 + \cdots + a_m - m + 2$ ist, nehmen wir zunächst an, sie sei größer als diese Zahl und machen klar, daß sie dann noch kleiner gemacht werden kann. Ist also die Ordnung von f um die Einheit kleiner als diese Zahl, so folgt

$$l \cdot f \equiv 0 \text{ mod. } (w_1, \cdots, w_{m-1}),$$

d. h. es wird ganzzahlige Formen $p_1, \cdots, p_{m-1}$ geben, so daß

$$l \cdot f = p_1 w_1 + \cdots + p_{m-1} w_{m-1}.$$

Da l relativ prim zu $w_1, \cdots, w_{m-2}, w_{m-1}$, so wird p_{m-1} zu den primären

Divisoren von $l, w, \cdots, w_{m-2}$ gehören, also nach Voraussetzung, da auch die Ordnung von p_{m-1} die Bedingung des Satzes XIX erfüllt, zum Ideal $w_1, \cdots, w_{m-2}, l$ gehören. Eine ganzzahlige Form q wird daher existieren, so daß

$$p_{m-1} \equiv ql \bmod. (w_1, \cdots, w_{m-2});$$

es wird also sein

$$lf - lq \cdot w_{m-1} \equiv 0 \bmod. (w_1, \cdots, w_{m-2})$$

und nach Satz I

$$f - qw_{m-1} \equiv 0 \bmod. (w_1, \cdots, w_{m-2}).$$

Nun sind aber f, q, w_{m-1} ganzzahlige Formen. Die linke Seite gehört also zum Ideal $w_1, \cdots, w_{m-2}$, welches ja ein ganzzahliger Modul ist, und demnach f zum Ideal

$$w_1, \cdots, w_{m-1}.$$

Die betreffende Ordnung kann also reduziert werden, solange

$$R > a_1 + \cdots + a_{m-1} - m + 2.$$

Satz XIX ist demnach richtig unter der Annahme des Induktionsschlusses im Bereiche von $m-1$ Variablen.

36. Seien nun $w_1, \cdots, w_{m-1}$ m Formen, von denen die letzte primitiv und linear, im Bereiche von m Variablen. Wir wählen ein System von $m-1$ ganzzahligen Linearformen, deren Determinante mit l die Einheit ergibt, und entwickeln $w_1, \cdots, w_{m-1}$ und f nach ihnen. So kommt

$$\begin{gathered} w_1 = w_1' + l \cdot w_1'' \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ w_{m-1} \equiv w_{m-1}' + l\, w_{m-1}'' \\ f \equiv f' + lf'', \end{gathered}$$

wobei die einfach gestrichelten Formen von l unabhängig sind. Da f zu den primären Divisoren von $w_1, \cdots, w_{m-1}, l$ gehört, so wird f mit irgend einer von l unabhängigen Form genügend hoher Ordnung multipliziert zum Ideal $(w_1, \cdots, w_{m-1}, l)$ gehören, f' wird also mit einer solchen Form multipliziert $(w_1', \cdots, w_{m-1}')$ zugehören, f' wird somit zu den primären Divisoren von $(w_1', \cdots, w_{m-1}')$ gehören. Ist nun noch die Ordnung von f nach der Bedingung von Satz XIX größer als

$$a_1 + \cdots + a_{m-1} + 1 - m,$$

so wird f' nach dem bereits Bewiesenen zum Ideal $(w_1', \cdots, w_{m-1}')$ gehören. Dies schließt aber offenbar ein, daß f zum Ideal $(w_1, \cdots, w_{m-1}, l)$ gehöre. Es ist damit durch Induktion klar gestellt, daß jede Form, deren Ordnung größer als $a_1 + \cdots + a_m - m$ und die zu den primären Divisoren von $(u_1, \cdots, u_m)$ gehört, zum Ideal $(u_1, \cdots, u_m)$ gehören muß.

Es sei f eine ganzzahlige Form, deren Ordnung $< a_1 + \cdots + a_m - m$, die apolar zu $\Omega(u_1, \cdots, u_m)$ ist und die zu den primären Divisoren d_i gehört. Wir wollen dann nachweisen, daß f zum Ideal $(u_1, \cdots, u_m)$ gehören muß. Dieser Satz ist offenbar richtig, wenn $m = 2$ und eine der Formen u_i eine primitive Linearform ist, denn dann ist eine zu $\Omega(u_1, u_2)$ apolare Form ein Multiplum dieser Linearform. Erweisen wir demnach die Behauptung durch Induktion, indem wir zeigen, daß der Satz richtig sein muß, wenn er richtig ist für $m-1$ Formen, von denen eine primitiv und linear ist, im Raume von $m-1$ Variablen.

Aus der letzteren Voraussetzung folgt zunächst, daß der Satz richtig ist für $m-1$ beliebige Formen von $m-1$ Variablen. Seien $w_1, \cdots, w_{m-1}$ die Formen, bereits so gewählt, daß $w_1, \cdots, w_{m-2}$ einen ganzzahligen Modul bilden. Sei l eine primitive zu $(w_1, \cdots, w_{m-1})$ relativ prime Linearform.

Ist f eine zu Ω konjugierte Form der Ordnung von Ω und gehört es zu den primären Teilen von $(w_1, \cdots, w_{m-1})$, so wird $l \cdot f$ zum Ideal $(w_1, \cdots, w_{m-1})$ gehören, d. h. es wird eine Identität existieren

$$l \cdot f = p_1 w_1 + \cdots + p_{m-1} w_{m-1},$$

wo die p_i ganzzahlige Formen. Auch wird, da f apolar zu $(w_1, \cdots, w_{m-1})$, eine nicht notwendig ganzzahlige Identität existieren

$$f = q_1 w_1 + \cdots + q_{m-1} w_{m-1},$$

also wird sein

$$(p_{m-1} - l q_{m-1}) w_{m-1} \equiv 0 \text{ mod. } (w_1, \cdots, w_{m-2})$$

und nach Satz I

$$p_{m-1} \equiv l q_{m-1} \text{ mod. } (w_1, \cdots, w_{m-2});$$

p_{m-1} wird daher apolar sein zu

$$\Omega(w_1, \cdots, w_{m-2}, l).$$

Auch wird p_{m-1} zu den primären Divisoren von $(w_1, \cdots, w_{m-2}, l)$ gehören, da

$$p_{m-1} w_{m-1} \equiv 0 \text{ mod. } (w_1, \cdots, w_{m-2}, l)$$

und w_{m-1} relativ prim zu $w_1, \cdots, w_{m-2}, l$. Mithin wird nach Voraussetzung p_{m-1} zum Ideal $(w_1, \cdots, w_{m-2}, l)$ gehören. Sei

$$p_{m-1} = q l + q_1 w_1 + \cdots + q_{m-2} w_{m-2}.$$

Setzen wir diesen Wert in die Identität

$$l \cdot f = p_1 w_1 + \cdots + p_{m-1} w_{m-1},$$

so folgt eine Identität der Gestalt

$$l(f - q w_{m-1}) = s_1 w_1 + \cdots + s_{m-2} w_{m-2}.$$

Nach Satz I ist

$$f - q w_{m-1} \equiv 0 \text{ mod. } (w_1, \cdots, w_{m-2}).$$

Doch $(w_1, \cdots, w_{m-2})$ war ein ganzzahliger Modul und f, q, w sind ganzzahlige Formen. Somit ist dann $f \equiv 0 \bmod. (w_1, \cdots, w_{m-1})$. Dies erweist die Richtigkeit der Behauptung für Formen f derselben Ordnung wie Ω und genau so kann man Schritt für Schritt die Richtigkeit der Behauptung erweisen für um die Einheit abnehmende Ordnungen. Der Satz ist also unter der Voraussetzung des Induktionsschlusses richtig für $m-1$ beliebige Formen im Bereiche von $m-1$ Variablen. Hieraus folgt nun wieder, daß der Satz richtig ist für $m-1$ Formen und eine primitive Linearform l im Bereiche von m Variablen. Seien die $m-1$ Formen $w_1, \cdots, w_{m-1}$. Entwickeln wir dieselben nach einem System von m linearen ganzzahligen Formen der Variablen, deren Determinante 1 ist und von denen l eine ist. Setzen wir

$$w_1 = w_1' + l w_1'',$$
$$\cdots\cdots\cdots$$
$$w_{m-1} = w_{m-1}' + l w_{m-1}'',$$
$$f = f' + l f'',$$

wo die $w_1', \cdots, w_{m-1}', f'$ von l unabhängig sind, so ist f' apolar zu

$$\Omega(w_1', \cdots, w_{m-1}'),$$

da aus der Apolarität von f zu $\Omega(w_1, \cdots, w_{m-1}, l)$ die Existenz der Kongruenzen $f \equiv 0 \bmod. (w_1, \cdots, w_{m-1}, l)$ und $f' \equiv 0 \bmod. (w_1', \cdots, w_{m-1}')$ folgt.

Da f zu den primären Divisoren des Moduls $(w_1, \cdots, w_{m-1}, l)$ gehört, so auch zu denen von $(w_1', \cdots, w_{m-1}', l)$.

Ein Multiplum genügend hoher Ordnung von f muß also zum Ideal $(w_1', \cdots, w_{m-1}', l)$ gehören, f' muß daher zu den primären Divisoren von $(w_1', \cdots, w_{m-1}')$ gehören. Mithin sind die notwendigen Voraussetzungen dafür erfüllt, daß f' zum Ideal $(w_1', \cdots, w_{m-1}')$ gehöre, und dies schließt offenbar ein, daß f zum Ideal $(w_1, \cdots, w_{m-1}, l)$ gehöre.

Der Beweis durch Induktion von Satz XIX für den Fall $h = m$ ist damit vollendet. Für $h < m$ folgt Satz XIX aber leicht aus obigem. Seien die primären Ideale h^{ter} Stufe von $u_1, \cdots, u_h$ mit $I_1, \cdots, I_j$ bezeichnet und sei

$$f \equiv 0 \bmod. [I_1, \cdots, I_j].$$

Seien $u_{h+1}, \cdots, u_m$ Formen mit unbestimmten Koeffizienten und von sehr hohen Ordnungen. f gehört alsdann zu den primären Divisoren von $u_1, \cdots, u_m$, da die primären Ideale, welche $(u_1, \cdots, u_h)$ außer den $I_1, \cdots, I_j$ noch haben mag, die also von höherer Stufe als h sind, durch fortgesetzten Schnitt mit relativ primen Formen u_{h+1}, u_{h+2} etc. schließlich zur Gesamtheit aller Formen werden müssen. Auch ist f apolar zu $\Omega(u_1, \cdots, u_m)$, da f, wenn nicht zum Ideal, doch nach Satz XI zum Modul $(u_1, \cdots, u_h)$ gehört. Somit gehört f nach dem, was bereits bewiesen, zum

Ideal $(u_1, \cdots, u_h, u_{h+1}, \cdots, u_m)$, was wegen der Höhe der Ordnungen von $u_{h+1}, \cdots, u_m$ darauf hinauskommt, daß f zum Ideal $(u_1, \cdots, u_h)$ gehört.

Satz XIX ist damit in allen seinen Teilen bewiesen.

37. Zum Schluß erweitern wir die Definition der Dedekindschen Funktion auf beliebige Ideale. Ist J irgend ein Ideal, so bedeute

$$DJ(R)$$

die Anzahl der Formen R^{ter} Ordnung, welche sämtlich dem J entsprechenden Modul angehören und für ganzzahlige Formen dieses Moduls ein vollständiges Restsystem in bezug auf J bilden. Ist

$$f_1, \cdots, f_n$$

ein Fundamentalsystem aller ganzzahligen Formen R^{ter} Ordnung des J entsprechenden Moduls und setzt man

$$u_1 f_1 + \cdots + u_n f_n = p_1 v_1 + \cdots + p_h v_h,$$

wo $v_1, \cdots, v_h$ eine Basis von J, $p_1, \cdots, p_h$ Formen mit unbestimmten Koeffizienten z_i, die $u_1, \cdots, u_n$ Unbestimmte sind, so sind die letzteren lineare Formen der z_i und jedem Wertsystem der u_i entsprechen Wertsysteme der z_i. Aus diesem Grunde verschwinden die Determinanten der Ordnung n der Linearformen u_i nicht sämtlich. Ihr größter gemeinschaftlicher Teiler ist nach den Sätzen von Frobenius-Smith gleich der Dedekindschen Funktion von J für die Ordnung R. Nur eine endliche Zahl der $e_1, \cdots, e_n$ des Systems der u_i können von 1 verschieden sein, und ihre Indizes sind für genügend große Werte der Ordnung R Polynome von R. Denn J ist nach Satz XIII gleich (M, d, r), wo M ein ganzzahliger Modul, d ein Divisor, r was man ein „endliches" Ideal nennen könnte und es zeigt sich auf die folgende Weise, daß

$$D(M, d) \cdot DJ = Dd$$

für alle Werte R ist. Es sei $A_1, \cdots, A_a$ ein vollständiges Restsystem R^{ter} Ordnung von (M, d). Ist dann B ein Glied des vollständigen Restsystems von d, das nicht in obigem enthalten, so ist

$$B \equiv A_i \bmod. (M, d)$$

für einen Index i. Mithin ist folgende Zerspaltung möglich

$$B - A_i = B' + B'',$$

wo $B' \equiv 0 \bmod. M$, $B'' \equiv 0 \bmod. d$. $B - B'' = A_i + B'$ ist also eine Form, die im vollständigen Restsystem von d B ersetzen könnte. Führen wir die Substitution aus. Es ist dann $A_i + B'$ für jeden Wert des Index i ein Glied des vollständigen Restsystems modulo d, da die Kongruenz $A_i + B' \equiv A_j \bmod. d$ zu $A_i \equiv A_j \bmod. (M, d)$ führen würde. Man kann

danach zeigen, daß das vollständige Restsystem von d sich in die Gestalt bringen lassen muß

$$\begin{array}{c} A_1 + B_1, \cdots, A_1 + B_b \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ A_a + B_1, \cdots, A_a + B_b, \end{array}$$

wo

$$A_i \equiv 0 \bmod. M.$$

Für einen bestimmten Index h wird nun $A_h + B_1, \cdots, A_h + B_b$ ein vollständiges Restsystem von J in bezug auf die Formen R^{ter} Ordnung von M sein. Offenbar ist nicht für verschiedene Indizes i, j

$$B_i \equiv B_j \bmod. d,$$

da

$$A_1 + B_i \quad \text{nicht} \quad \equiv A_1 + B_j \bmod. d.$$

Ist F irgend eine Form R^{ter} Ordnung von M, so wird es Indizes h, k geben, so daß

$$F \equiv A_h + B_k \bmod. d.$$

Der Index h wird immer derselbe sein, denn aus obigem folgt

$$A_h \equiv 0 \bmod. (M, d).$$

$A_h + B_1, \cdots, A_h + B_b$ ist also in der Tat ein vollständiges Restsystem der Formen von M in bezug auf J. Ihre Anzahl ist b. Es war aber

$$D(M, d) = a, \quad Dd = a \cdot b.$$

Die Behauptung ist damit klar gestellt.

Die kleinste Zahl, mit der multipliziert Formen von M dem Ideal J angehören, ist für genügend große Werte von R jedenfalls nicht größer als die kleinste d zugehörige Zahl. Hieraus und aus Schlüssen, die den schon früher angestellten parallel laufen, ergibt sich die Richtigkeit des folgenden Satzes:

Satz XX. „Die Gesamtheit der Formen R^{ter} Ordnung eines Ideals J ist darstellbar in der Gestalt

$$\begin{aligned} A(u_1 f_1 + \cdots + u_a f_a) + B(u_{a+1} f_{a+1} + \cdots + u_b f_b) + \cdots \\ + N(u_{k+1} f_{k+1} + \cdots + u_n f_n). \end{aligned}$$

Hierbei bedeuten $f_1, \cdots, f_n$ Formen, die Teil eines ganzzahligen Fundamentalsystems aller Formen R^{ter} Ordnung bilden können. Die $u_1, \cdots, u_n$ sind beliebige ganze Zahlen, $A, B, \cdots, N$ sind ein System sich mit R nicht ändernder ganzer Zahlen, von denen jede durch die vorhergehende teilbar ist, und $a, b, \cdots, n$ sind Funktionen von R, welche für genügend große Werte von R gleich Polynomen von R sind."

Kapitel III.

Erweiterung auf Potenzreihen.

38. Die Grundlagen der bisherigen Untersuchung seien nun erweitert auf den Bereich der analytischen Funktionen. Auch dann bleiben viele der bisherigen Ergebnisse bestehen und andere fügen sich an, welche für die Erkenntnis gewisser Beziehungen sowohl in der Funktionentheorie wie in der Algebra von Bedeutung sind.

Der Bereich der Funktionen sei der der Potenzreihen von $m-1$ Veränderlichen

$$x_1, x_2, \cdots, x_{m-1},$$

welche um den gegebenen Punkt

$$P \equiv x_1 = x_2 = \cdots = x_{m-1} = 0$$

herum einen endlichen, wenn auch beliebig kleinen Konvergenzbereich haben, so daß sich also positive von Null verschiedene Größen

$$e_1, e_2, \cdots, e_{m-1}$$

angeben lassen, derart, daß die Werte

$$|x_1| < e_1, \ |x_2| < e_2, \cdots, |x_{m-1}| < e_{m-1}$$

dem Konvergenzbereich der hier betrachteten Potenzreihen angehören.

Sind $f_1, f_2, \cdots, f_h$ derartige Potenzreihen, welche sämtlich in P verschwinden, so heiße die Gesamtheit aller Potenzreihen

$$A_1 f_1 + \cdots + A_h f_h,$$

wo die $A_1, \cdots, A_h$ ganz beliebige Potenzreihen der $x_1, \cdots, x_{m-1}$ sind, ein um P analytischer Modul, oder kurz ein P-Modul. Ist E irgend eine in P nicht verschwindende Potenzreihe

$$E = 1 + ax_1 + bx_2 + \cdots + cx_1x_2 + \cdots \text{ in inf.},$$

so ist

$$\frac{1}{E} = 1 - (ax_1 + bx_2 + \cdots + cx_1x_2 + \cdots)$$
$$+ (ax_1 + bx_2 + \cdots + cx_1x_2 + \cdots)^2 - \cdots$$

ebenfalls in derselben Weise entwickelbar. In bezug auf P-Moduln verhalten sich daher Faktoren der Gattung E wie Einheiten. Ist M ein P-Modul und ist

$$F \,.\, E \equiv 0 \text{ mod. } M,$$

so ist auch

$$F \equiv 0 \text{ mod. } M.$$

Es sei nun angesetzt

$$f_1 = \sum_{0 \cdots 0}^{\infty \cdots \infty} {}^{n_1, \cdots, n_{m-1}} f^{(1)}_{n_1, \cdots, n_{m-1}} x_1^{n_1} \cdots x_{m-1}^{n_{m-1}}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$f_h = \sum_{0 \cdots 0}^{\infty \cdots \infty} {}^{n_1, \cdots, n_{m-1}} f^{(h)}_{n_1, \cdots, n_{m-1}} x_1^{n_1} \cdots x_{m-1}^{n_{m-1}}.$$

Hier bedeuten also die $f^{(i)}_{n_1, \cdots, n_{m-1}}$ für jedes System der Indizes gegebene Größen, nur eingeschränkt durch Konvergenzbedingungen in einem endlichen, doch beliebig kleinen Bereich. Unter derselben Einschränkung sei angesetzt

$$A_i = \sum_{0 \cdots 0}^{\infty \cdots \infty} {}^{n_1, \cdots, n_{m-1}} a^{(i)}_{n_1, \cdots, n_{m-1}} x_1^{n_1} \cdots x_{m-1}^{n_{m-1}},$$

wo die $a^{(i)}_{n_1, \cdots, n_{m-1}}$ konstante, jedoch unbestimmte Größen bedeuten. Wir setzen nun an

$$F = \sum_{0 \cdots 0}^{\infty \cdots \infty} {}^{n_1, \cdots, n_{m-1}} y_{n_1, \cdots, n_{m-1}} x_1^{n_1} \cdots x_{m-1}^{n_{m-1}},$$

indem wir mit $y_{n_1, \cdots, n_{m-1}}$ ein System Variabler bezeichnen, und suchen die Beziehungen, welche zwischen diesen Variablen obwalten müssen, damit eine Beziehung der Art

$$F = A_1 \cdot f_1 + \cdots + A_h \cdot f_h$$

möglich sei. Durch Vergleichung der Koeffizienten der Potenzprodukte $x_1^{n_1} \cdots x_{m-1}^{n_{m-1}}$ ergibt sich aus obiger Gleichung eine beliebig weit fortsetzbare Reihe linearer Identitäten

$$y_{0, \cdots, 0} = 0$$

$$y_{1, 0, \cdots, 0} = a^{(1)}_{0, \cdots, 0} f^{(1)}_{1, 0, \cdots, 0} + \cdots + a^{(h)}_{0, \cdots, 0} f^{(h)}_{1, 0, \cdots, 0}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$y_{n_1, \cdots, n_{m-1}} = \sum a^{(i)}_{g, \cdots, k} f^{(i)}_{g', \cdots, k'},$$

wo die Summation auszudehnen ist über alle Gruppen positiver ganzer Zahlen, die 0 mit eingeschlossen, von $g, \cdots, k, g', \cdots, k'$, für welche

$$g + g' = n_1, \cdots, k + k' = n_{m-1},$$

und über alle Indizes i von 1 bis h.

Wir nennen

$$n_1 + \cdots + n_{m-1} = r$$

die „Ordnung" einer Variablen $y_{n_1, \cdots, n_{m-1}}$, eliminieren die Unbestimmten a aus obigen Gleichungen, indem wir sukzessive erst alle Gleichungen

obiger Art der Ordnung $r = 0$, dann $r = 1$, dann $r = 2, \cdots$ betrachten, und erhalten auf diese Weise ein System linearer Beziehungen für die Variablen y

$$y_{0,0,\cdots,0} = 0$$

$$k \cdot y_{1,0,\cdots,0} + l \cdot y_{0,1,\cdots,0} + \cdots + n \cdot y_{0,0,\cdots,1} = 0$$

etc. etc.,

welche die „Noetherschen Bedingungen" des P-Moduls $(f_1, \cdots, f_h)$ genannt werden sollen. Je nach der Maximalordnung der y, welche auf der linken Seite einer Noetherschen Bedingung stehen, werden wir letztere nach Ordnungen einteilen, so daß wir von der Gruppe der Noetherschen Bedingungen des P-Moduls der Ordnung $0, 1, 2, \cdots, r \cdots$ sprechen können. Die linke Seite einer Noetherschen Bedingung der Ordnung r des Moduls werden wir eine Noethersche Form der Ordnung r des P-Moduls nennen, und da es im allgemeinen verschiedene Noethersche Formen der Ordnung r desselben Moduls gibt, so werden wir von der (linearen) Schar solcher Noetherschen Formen als von der Gesamtheit der überhaupt möglichen Noetherschen Formen der Ordnung r des gegebenen P-Moduls sprechen.

39. Wenn eine Funktion F dem P-Modul M angehört, so ist dasselbe der Fall mit $t \cdot F$, wo t eine Potenzreihe um P mit beliebigen Koeffizienten bedeutet. Diese einfache Bemerkung klärt uns über das wesentlichste Merkmal der Struktur des unendlichen Systems der Noetherschen Bedingungen desselben P-Moduls auf. Denn da die Multiplikation von F mit t in ihrer Wirkung auf die Koeffizienten y einer linearen Transformation derselben gleichkommt, so ergeben sich durch Einsetzen dieser transformierten Werte für die ursprünglichen y wichtige Beziehungen zwischen den Scharen Noetherscher Formen.

Es sei N_r die Gesamtschar Noetherscher Formen r^{ter} Ordnung von M. Ersetzen wir

$$y_{n_1, \cdots, n_{m-1}} \quad \text{durch} \quad \sum t_{g, \cdots, k} \cdot y_{g', \cdots, k'},$$

die Summation ausgedehnt über alle Indexsysteme $g, \cdots, k, g', \cdots, k'$, für welche

$$g + g' = n_1, \cdots, k + k' = n_{m-1},$$

so wird durch diese Transformation F übergeführt in $t \cdot F$ und N_r übergeführt in einen Ausdruck derselben Ordnung r, welcher, nach den $t_{g, \cdots, k}$ entwickelt, geschrieben werden kann

$$N_r \cdot t_{0, \cdots, 0} + A_1 \cdot t_{1,0,\cdots,0} + B_1 \cdot t_{0,1,\cdots,0} + \cdots + A_2 \cdot t_{1,1,0,\cdots,0} + \cdots.$$

Dabei bedeuten die $A_1, B_1, \cdots, A_2, \cdots$ lineare Formen der y allein, A_1 der $(r-1)^{\text{ten}}$ Ordnung, A_2 der $(r-2)^{\text{ten}}$ Ordnung etc. Wenn nun $N_r = 0$

eine notwendige Bedingung ist für alle Formen F, die M angehören, so folgt, da ja die t sämtlich Unbestimmte sind, daß auch

$$A_1 = 0,\ B_1 = 0, \cdots, A_2 = 0, \cdots$$

Bedingungen sind, die eine Form des Moduls M notwendig erfüllen muß.

Jede Schar S von Noetherschen Bedingungen r^{ter} Ordnung zieht daher Scharen von Noetherschen Bedingungen kleinerer Ordnung als r notwendig nach sich. Die letzteren sind durch den eben beschriebenen Prozeß aus S zu gewinnen und heißen die „Dependenzen von S".

Es besteht nun der

Satz XXI: „Jedes System von Noetherschen Bedingungen, welches derart ist, daß mit jeder Noetherschen Bedingung auch alle ihre Dependenzen im System enthalten sind, bestimmt einen analytischen P-Modul."

Dabei verstehen wir unter einem analytischen P-Modul eine Menge von Potenzreihen um P, derart beschaffen, daß mit zwei Individuen p und q derselben auch $ap + bq$ in der Menge enthalten sei, wo a und b beliebige Potenzreihen um P.

Der Beweis des obigen Satzes ist sehr einfach. Seien die Scharen Noetherscher Bedingungen aller Ordnungen

$$N_0 = 0,\ N_1 = 0,\ N_2 = 0, \cdots, N_r = 0, \cdots$$

und sei die Gesamtheit der Potenzreihen betrachtet, die denselben genügen. Ist p ein Individuum dieser Menge, ist a irgend eine Potenzreihe, so werden durch Bildung von ap die Koeffizienten von p einer Transformation unterworfen, die N_r überführt in eine Summe von Noetherschen Bedingungen, die sämtlich in dem System $N_0, N_1, \cdots, N_r$ enthalten sind. Folglich ist mit p auch ap in der oben bestimmten Menge von Funktionen enthalten. Auch sind sämtliche den Koeffizienten der Potenzreihen auferlegte Bedingungen lineare. Somit ist, wenn p und q Individuen der Menge, dasselbe der Fall mit $ap + bq$.

Umgekehrt geht auch aus obiger Analyse hervor, daß das System der Noetherschen Bedingungen, welche einem gegebenen P-Modul M angehören, die im obigen Satze angegebene Eigenschaft haben muß.

40. Es gilt nun für P-Moduln das dem Theorem I (Kap. II, Nr. 16) für Moduln entsprechende Theorem:

Satz XXII: „Sind

$$f_1, f_2, \cdots, f_n \cdots$$

eine unendliche Reihe von Potenzreihen um P, so läßt sich immer eine Zahl k bestimmen, derart, daß für jeden Index $i > k$ Potenzreihen um P

$$p_1, p_2, \cdots, p_k$$

existieren, die eine Beziehung

$$f_i = p_1 \cdot f_1 + \cdots + p_k \cdot f_k$$

befriedigen."

Das Prinzip des Beweises dieses Satzes beruht auf einem anderen wichtigen Satze:

Satz XXIII: „Ist

$$f = \sum_{0 \cdots 0}^{\infty \cdots \infty} {}_{n_1, \cdots, n_{m-1}} c_{n_1, \cdots, n_{m-1}} x_1^{n_1} \cdots x_{m-1}^{n_{m-1}}$$

irgend eine gegebene Potenzreihe, so läßt sich immer eine in

$$x_1 = 0, \cdots, x_{m-1} = 0$$

nicht verschwindende Potenzreihe G angeben, derart, daß $G \cdot f$ eine Potenzreihe, in der die Potenzen einer der Variablen nicht über einen angebbaren Grad steigen."

Dieser Satz ist von Weierstraß gegeben und bewiesen worden (Math. Werke, Bd. II, Nr. 10). Der Beweis könnte auch durch Koeffizientenvergleichung und, bezüglich der Konvergenz von G, nach dem Cauchyschen Verfahren für die Integrale analytischer Differentialgleichungen geführt werden.

Aus Satz XXIII ist der Beweis des Satzes XXII unschwer zu erbringen. Dieser Satz ist offenbar richtig für Potenzreihen nur einer Variablen, aus dem schon von Hilbert angeführten Grunde. Führen wir nun den zu erbringenden Nachweis durch Induktion, genau wie Hilbert, so können wir durch die Darstellung jeder der Funktionen $f_1, f_2, \cdots, f_n, \cdots$ in der durch den Satz XXIII als möglich erwiesenen Gestalt

$$f_n = F_n \cdot (x^g + x^{g-1} A_n + x^{g-2} B_n + \cdots)$$

(wo F_n eine in P nicht verschwindende Potenzreihe, x eine Variable, $A_n, B_n, \cdots$ Potenzeihen der übrigen $m-2$ Variablen), auch den übrigen Schlüssen von Hilbert genau folgen.

41. Auch der Irreduzibilitätsbegriff hat eine Bedeutung in der Algebra der Potenzreihen um P, vorausgesetzt nur, daß in P nicht verschwindende Potenzreihen als Einheiten betrachtet werden.

Danach heißt eine Potenzreihe f um P irreduzibel, wenn es nicht möglich ist, zwei in P verschwindende Potenzreihen A, B zu finden, so daß identisch $F = A \cdot B$. Es besteht der

Satz XXIV: „Jede Potenzreihe um P läßt sich nur auf *eine* Weise in der Gestalt

$$f = A^a \cdot B^b \cdots C^c$$

darstellen, wo $A, B, \cdots, C$ irreduzible Potenzreihen um P sind."

Dabei ist also eine Potenzreihe um P jeder anderen, die sich von ihr nur um einen in P nicht verschwindenden Potenzreihenfaktor unter-

scheidet, äquivalent gesetzt. Für Funktionen *einer* Variablen ist die Behauptung augenscheinlich, da die Variable selbst die einzige irreduzible Form, und jede Potenzreihe einer Potenz derselben äquivalent ist. Man beweist Satz XXIV durch Induktion, indem man nach Satz XXIII jede Potenzreihe einer anderen der Gestalt

$$x^g + x^{g-1} f_1 + x^{g-2} f_2 + \cdots + f_g$$

äquivalent setzen kann, unter $f_1, \cdots, f_g$ Potenzreihen der $m-2$ anderen Variablen verstanden, und dann den Schlüssen der Algebra folgt, die den Irreduzibilitätssatz für Formen erweisen, und die im letzten Grunde auf dem ja auch hier anwendbaren Euklidischen Verfahren zur Feststellung des größten gemeinsamen Teilers zweier Formen beruhen.

Ist f irgend eine irreduzible Potenzreihe, so definiert $f=0$ eine P enthaltende Oberfläche, und zwar als die ganze Mannigfaltigkeit von Wertsystemen $x_1, \cdots, x_{m-1}$, die $f=0$ machen und deren absolute Werte kleiner sind als eine angebbare vom Konvergenzbezirk der Reihe f abhängige Größe. Diese Oberfläche bei P wird ebenso wie f selbst irreduzibel genannt werden.

Zwei irreduzible Oberflächen bei P „schneiden" sich in einem bei P analytischen Gebilde zweiter Stufe, auf welches der Irreduzibilitätsbegriff ebenso anwendbar ist, wie auf die entsprechenden algebraischen Gebilde.

Wir ersetzen die Variablen $x_1, \cdots, x_{m-1}$ durch eine lineare homogene Transformation mit unbestimmten Koeffizienten, entwickeln die beiden irreduziblen Potenzreihen nach Potenzen einer der Variablen gemäß Satz XXIII, das Zeichen $=$ im Sinne der Äquivalenz deutend,

$$f_1 = x^g + x^{g-1} A_1 + \cdots,$$
$$f_2 = x^h + x^{h-1} A_2 + \cdots,$$

bilden die Resultante von f_1, f_2 nach x

$$\text{Res.}\,(f_1, f_2) = F,$$

wo F also eine Potenzreihe der übrigen $m-2$ Variablen, und bestimmen die irreduziblen Teiler von F. Jedem dieser verschiedenen irreduziblen Teiler entspricht, genau wie in den Betrachtungen des Satzes IV, ein Gebilde zweiter Stufe und der Mannigfaltigkeit $m-2$. Überhaupt lassen sich alle Definitionen und Schlüsse des Satzes IV hier wiederholen. Es zeigt sich, daß jede analytische Konfiguration bei P, definiert durch ein System von Potenzreihen bei P, auflösbar ist in eine Gruppe irreduzibler analytischer Gebilde bei P und zwar nur auf *eine* Weise.

42. Satz XXV. „Ist die Anzahl der Noetherschen Bedingungen eines Moduls in einem Punkte P endlich, so ist die Mannigfaltigkeit der den Formen des P-Moduls gemeinsamen Gebilde $= 1$."

Wir erweisen diesen Satz, indem wir annehmen, daß die Formen eines P-Moduls Gebilde höherer Mannigfaltigkeit als 1 gemeinsam besitzen, und dann dartun, daß der P-Modul infolgedessen beliebig viele Noethersche Bedingungen erfüllt. Sei ein Gebilde G bei P allen Formen eines P-Moduls M gemeinsam. Es wird möglich sein, die Punkte von G in der Nachbarschaft von P durch mindestens einen Parameter k analytisch darzustellen:

$$\begin{aligned} x_1 &= a_{1,1}k + a_{1,2}k^2 + \cdots \\ x_2 &= a_{2,1}k + a_{2,2}k^2 + \cdots \\ &\cdots\cdots\cdots\cdots \\ x_{m-1} &= a_{m-1,1}k + a_{m-1,2}k^2 + \cdots \end{aligned}$$

Da jede Form F von M G enthält, so ist für obige Werte von $x_1, \cdots, x_{m-1}$ identisch

$$F(x_1, \cdots, x_{m-1}) = 0$$

oder nach dem Taylorschen Satz

$$\frac{\partial F(0,\cdots,0)}{\partial x_1} x_1 + \frac{\partial F(0,\cdots,0)}{\partial x_2} x_2 + \cdots = 0,$$

$$\frac{\partial F(0,\cdots,0)}{\partial x_1}(a_{1,1}k + a_{1,2}k^2 + \cdots) + \frac{\partial F(0,\cdots,0)}{\partial x_2}(a_{2,1}k + \cdots) + \cdots = 0.$$

Entwickeln wir diesen Ausdruck nach Potenzen von k in der Gestalt

$$Ak + Bk^2 + \cdots,$$

so folgt aus obiger Beziehung

$$A = 0,\ B = 0,\ \cdots$$

Die $A, B, \cdots$ sind Ausdrücke der Form

$$l\frac{\partial F(0,\cdots,0)}{\partial x_1} + h \cdot \frac{\partial F(0,\cdots,0)}{\partial x_2} + \cdots,$$

wo $l, h, \cdots$ Konstanten, und die $\frac{\partial F(0,\cdots,0)}{\partial x_1}$ etc. sind nichts anderes als was früher mit $y_{n_1,\cdots,n_{m-1}}$ bezeichnet war. Mithin erhält man in der Tat aus der Tatsache heraus, daß eine beliebige Form F von M ein Gebilde höherer Mannigfaltigkeit als 1 bei P enthält, unendlich viele Noethersche Bedingungen für die Formen von M und Satz XXV muß daher richtig sein.

43. Es sind nun alle Folgerungen des Satzes VII möglich, und es zeigt sich, daß, wenn in genauester Analogie zu den Entwicklungen des Kap. II die Begriffe des Prim-P-Moduls und primären P-Moduls eingeführt werden, jeder P-Modul M entwickelbar ist in der Gestalt

$$M = [D_1, D_2, \cdots, D_j, r],$$

wo $D_1, \cdots, D_j$ primäre P-Moduln und r ein P-Modul, dessen Formen kein Gebilde außer P gemein haben.

Satz XXVI. „Die Mannigfaltigkeit der Schar von Noetherschen Bedingungen r^{ter} Ordnung eines P-Moduls M nennen wir die Noether-Hilbertsche Funktion von M. Ist M ein P-Modul der Mannigfaltigkeit h, so ist für genügend große Werte von r die Noether-Hilbertsche Funktion von M darstellbar als ein Polynom $(h-2)^{\text{ten}}$ Grades von r."

Jedem P-Modul M entspricht im Bereiche des Raumes $x_1, \cdots, x_{m-1}$ ein Modul M' durch folgende Festsetzung. M' enthalte alle Formen in $x_1, \cdots, x_{m-1}$, welche den Term niedrigster Ordnung der Entwicklung eines Individuums von M bilden können. Daß die Gesamtheit solcher Formen einen Modul M' bildet, ergibt sich leicht. Denn genügen p wie q der Definition der Formen von M', so existieren Individuen $\mathfrak{p}$ und $\mathfrak{q}$ von M, derart daß

$$\mathfrak{p} = p + p' + p'' + \cdots,$$
$$\mathfrak{q} = q + q' + q'' + \cdots,$$

wo $p', p'', \cdots$ von höherer Ordnung als p, $q', q'', \cdots$ von höherer Ordnung als q. Da nun, wenn a und b homogene Formen in $x_1, \cdots, x_{m-1}$, $ap + bq$ der Anfangsterm von $a\mathfrak{p} + b\mathfrak{q}$, so gehört auch $ap + bq$ zur Menge M'.

Die Formen von M' der Ordnung r lassen sich nun erhalten, indem in einer allgemeinen Potenzreihe F alle Koeffizienten y der Ordnung $< r$ gleich Null gesetzt werden und im übrigen die y den Noetherschen Bedingungen von M unterworfen werden. Daher ist die Anzahl der Bedingungen, denen die Formen r^{ter} Ordnung von M' genügen müssen, gleich der Anzahl der linear-independenten Noetherschen Bedingungen von M der Ordnung r d. h.

$$(N, H)\, M(r) = HM'(r):$$

die Noether-Hilbertsche Funktion von M ist gleich der Hilbertschen Funktion von M'.

Wir müssen nun nachweisen, daß, wenn u eine relativ prime Form zu M', und wenn der dem Modul (M, u) in obiger Weise entsprechende Modul mit $(M, u)'$ bezeichnet wird, für genügend große Werte von r

$$H(M, u)'(r) = H(M', u)(r).$$

Dies zeigt sich wie folgt. Alle Individuen von (M, u) haben die Gestalt

$$F + G \cdot u,$$

wo $F \equiv 0 \bmod. M$ und G eine beliebige Potenzreihe von P. Entwickeln wir diese Potenzreihe nach Termen aufsteigender Ordnung, so kommt

$$F + G \cdot u = p + p' + p'' + \cdots + g_0 \cdot u + g_1 \cdot u + g_2 \cdot u + \cdots,$$

wo $p + p' + p'' + \cdots$ die Terme aufsteigender Ordnung der Entwicklung von F, mit unbestimmten Koeffizienten versehen.

Ist p der Ordnung r, u der Ordnung a, so sei g_i eine Form mit unbestimmten Koeffizienten der Ordnung $r - a + i$. Offenbar gehört jedes $p + g_0 \cdot u$ dem Modul $(M, u)'$ an, außerdem aber noch der Term niedrigster Ordnung der Entwicklung von $F + G \cdot u$, wenn $p + g_0 \cdot u$ identisch verschwindet.

Nun ist $p \equiv 0 \bmod. M'$. Auch war u relativ prim zu M'. Aus $p + g_0 \cdot u \equiv 0 \bmod. M'$, für irgendwelche bestimmte Werte oder Koeffizienten von p und g_0, folgt daher $g_0 \cdot u \equiv 0 \bmod. M'$ und $g_0 \cdot v \equiv 0 \bmod. M'$, wo v eine Form mit unbestimmten Koeffizienten und von genügend hoher Ordnung. Es besteht daher eine M angehörige Reihe, deren erster Term $g_0 \cdot v$ ist, etwa

$$f = g_0 \cdot v + h_1 + h_2 + \cdots$$

Sind daher p und g_0 so bestimmt, daß

$$p + g_0 \cdot u = 0,$$

so ist in der Entwicklung von

$$vF + fu = v(p + g_0 \cdot u) + (vp' + h_1 \cdot u) + (vp'' + h_2 \cdot u) + \cdots$$

$vp' + h_1 \cdot u$ das erste Glied der Entwicklung, d. h.

$$vp' + h_1 \cdot u \equiv 0 \bmod. M',$$
$$vp' \qquad\quad \equiv 0 \bmod. (M', u).$$

Andrerseits ist unter denselben Umständen in der Entwicklung von

$$F + g \cdot u = (p + g_0 \cdot u) + (p' + g_1 \cdot u) + \cdots$$

$p' + g_1 \cdot u$ der erste Term, also

$$p' + g_1 \cdot u \equiv 0 \bmod. (M, u)',$$

und alle Terme von $(M, u)'$, die sich nicht sogleich in der Gestalt $p + g_0 \cdot u$, wo $p \equiv 0 \bmod. M'$, ergeben, lassen sich so darstellen, wenn nicht p' und g_1 solche Koeffizienten haben, daß

$$p' + g_1 \cdot u = 0.$$

Diese Möglichkeit vorderhand beiseite lassend, ersehen wir aus

$$p' + g_1 \cdot u \equiv 0 \bmod. (M, u)' \quad \text{und} \quad v(p' + g_1 \cdot u) \equiv 0 \bmod. (M', u),$$

daß jede Form, welche $(M, u)'$ angehört, mit einer unbestimmten Form genügend hoher Ordnung multipliziert (M', u) angehört. Dieser Schluß ist nur für solche Formen nicht gerechtfertigt, die erste Terme einer Entwicklung von $F + G \cdot u$ sind, in denen identisch $p + g_0 \cdot u = 0$, $p' + g_1 \cdot u = 0$. Alsdann aber ist

$$g_0 \cdot v \equiv 0 \bmod. M',$$
$$g_1 \cdot v \equiv 0 \bmod. M'.$$

Es existiert daher ein Individuum von M mit der Entwicklung

$$g_1 \cdot v + l_1 + l_2 + \cdots,$$

und ein anderes mit der Entwicklung

$$vp + vp' + vp'' + \cdots + u(g_0 \cdot v + h_1 + h_2 + \cdots) + u(g_1 \cdot v + l_1 + \cdots)$$

d. h. da

$$p + g_0 \cdot u = 0, \quad p' + g_1 \cdot u = 0,$$

mit

$$h_1 \cdot u + (vp'' + ul_1) + \cdots;$$

hieraus

$$h_1 \cdot u \equiv 0 \text{ mod. } M'$$

und, da u relativ prim zu M',

$$h_1 \cdot v \equiv 0 \text{ mod. } M'.$$

Ein Glied von M hat somit die Entwicklung

$$h_1 \cdot v + k_1 + k_2 + \cdots$$

und eines

$$v[l_1 \cdot u + (vp'' + ul_1) + \cdots] - u(h_1 \cdot v + k_1 + \cdots)$$

d. h.

$$(v^2 p'' + au) + \cdots$$

Dies zeigt, daß $v^2 p'' + au \equiv 0$ mod. M' und $v^2 p'' \equiv 0$ mod. (M', u).

Andrerseits ist $p'' + g_2 \cdot u$ der allgemeine Ausdruck derjenigen Individuen von $(M, u)'$, welche erste Terme einer Entwicklung von $F + G \cdot u$ sind, für die identisch $p + g_0 \cdot u = 0$, $p' + g_1 \cdot u = 0$. Für diese zeigt sich also, daß sie, mit dem Quadrat einer unbestimmten Form genügend hoher Ordnung multipliziert, notwendig (M', u) angehören. So können wir beliebig weit fortschreiten, indem wir noch $p'' + g_2 \cdot u = 0$ setzen und in analoger Weise wie bisher verfahren.

Nach einer endlichen Anzahl von Operationen müssen wir aber mit obigem Prozeß jedes Glied von $(M, u)'$ jeder gegebenen Ordnung R finden, da ja die Ordnungen der Anfangsterme bei obigem Prozeß immerfort wachsen.

Vergegenwärtigen wir uns nun die Darstellung von $(M, u)'$ wie (M', u) nach Satz VII, so folgt aus der Unbestimmtheit der Koeffizienten von v in Verbindung mit obigem Ergebnis, daß $(M, u)'$ und (M', u) in ihren primären Teilern übereinstimmen müssen, also die Gültigkeit der aufgestellten Behauptung. Die übrigen Schlüsse sind einfacher Natur. Es habe zunächst M die Mannigfaltigkeit 2. Ist dann u eine Linearform mit unbestimmten Koeffizienten, welche also das den Formen von M gemeinsame Gebilde nicht enthält, so ist nach Satz XXV $H(M, u)'(r)$ für genügend große Werte von r gleich 0. Andrerseits ist für genügend große Werte von r

$$H(M, u)'(r) = H(M', u)(r) = \Delta_1 HM'(r),$$

mithin

$$\Delta_1 HM'(r) = 0,$$

$HM'(r)$ eine Konstante.

Der Wert dieser Konstanten kann nicht 0 sein, da

$$(N, H)\, M(r) = H M'(r)$$

und da M Noethersche Bedingungen beliebig hoher Ordnung, wie wir bereits gesehen haben, wirklich besitzt. Hat M die Mannigfaltigkeit 3, so, unter denselben Umständen wie oben, (M, u) diejenige 2. Mithin folgt genau wie oben

$$\Delta_1 H M'(r) = a,$$

wo a eine nicht verschwindende Konstante, und

$$H M'(r) = ar + b,$$

wo b eine neue Konstante. Der Beweis des Satzes durch Induktion ist damit klargelegt.

44. Damit sind alle Vorbedingungen erfüllt, um die Schlüsse des Satzes X auch in der Theorie der P-Moduln wiederholen zu können.

Es sei nun M ein beliebiger Modul, P irgend ein seinen Formen gemeinsamer Punkt. Alsdann wollen wir mit M_P die Gesamtheit der *Formen* bezeichnen, die dem Modul M als P-Modul betrachtet zugehören, und ihn mit dem Namen „Noetherscher Modul von M bei P" belegen. Für solche Moduln gilt der fundamentale

Satz XXVII. „Ist $f \equiv 0$ mod. M_P, so gibt es immer eine Form Φ, welche P nicht enthält, und derart, daß

$$f \cdot \Phi \equiv 0 \text{ mod. } M."$$

Zunächst beweisen wir einen Hilfssatz: „Ist Q ein primärer Modul, und ist P irgend ein Punkt des zu einem Primmodul P gehörigen Gebildes, so ist $Q_P = Q$." Besteht das Gebilde von Q nur aus dem Punkte $P(x_1 = 0, \cdots, x_{m-1} = 0)$, so sind die definierenden Bedingungen der Potenzreihen von Q_P mit einer endlichen Anzahl Noetherscher Bedingungen erschöpft. Ist $u_1, \cdots, u_h$ eine Basis von Q, so ist Q_P definiert als die Gesamtheit der Formen, die in der Gestalt $A_1 \cdot u_1 + \cdots + A_h \cdot u_h$ darstellbar sind, $A_1, \cdots, A_h$ als Potenzreihen um P verstanden.

Ist nun $f = A_1 u_1 + \cdots + A_h u_h$ eine Form von Q_P und brechen wir die $A_1, \cdots, A_h$ bei den Termen ab, die P als R-fachen Punkt enthalten, so läßt sich f darstellen in der Gestalt

$$f = (a_1 u_1 + \cdots + a_h u_h) + u,$$

wo u P als mindestens $(R+1)$-fachen Punkt enthält. Nach Satz X läßt sich R bestimmen, groß genug, daß $u \equiv 0$ mod. Q. Also ist $f \equiv 0$ mod. Q und in der Tat

$$Q_P = Q,$$

wenn die Mannigfaltigkeit von Q gleich 1 ist.

Wir führen nun den Nachweis des aufgestellten Satzes durch In-

duktion, indem wir annehmen, daß er bereits bewiesen sei für Moduln der Mannigfaltigkeit $h-1$ und ihn auf Moduln der Mannigfaltigkeit h erweitern.

Ist der Hilfssatz für Moduln der Mannigfaltigkeit $h-1$ richtig, so auch Satz XXVII unter derselben Einschränkung. Denn sei nach Satz VII

$$M = [Q_1, Q_2, \cdots, Q_j, R]$$

und ist P in den zu $Q_a, Q_b, \cdots, Q_c$ gehörigen Gebilden enthalten, so enthalten die Noetherschen Bedingungen von M_P sicherlich diejenigen von $Q_{a,P}, Q_{b,P}, \cdots, Q_{c,P}$, also auch die von $[Q_{a,P}, \cdots, Q_{c,P}]$. Andrerseits, wenn f eine Form von $[Q_{a,P}, \cdots, Q_{c,P}]$, so ist, da $Q_a, \cdots, Q_c$ höchstens die Mannigfaltigkeit $h-1$ haben, nach Voraussetzung $Q_{a,P} = Q_a, \cdots, Q_{c,P} = Q_c$, und wenn Φ irgend eine Form des Moduls $[Q_1, Q_2, \cdots, Q_j, R]$, wo in der Klammer nur die $Q_a, Q_b, \cdots, Q_c$ fehlen, ist daher

$$f \cdot \Phi \equiv 0 \text{ mod. } M,$$

mithin

$$f \equiv 0 \text{ mod. } M_P,$$

da Φ P nicht zu enthalten braucht.

Modul $[Q_a, \cdots, Q_c]$ enthält also auch M_P. M_P ist somit identisch mit $[Q_a, \cdots, Q_c]$ und der aufgestellte Satz ist daher richtig unter der gemachten Annahme.

Sei nun Q ein primärer Modul der Mannigfaltigkeit h, u eine beliebige P enthaltende Form. Ist f eine Form von Q_P, so ist sie es auch a fortiori von $(Q, u)_P$. (Q, u) ist aber ein Modul der Mannigfaltigkeit $h-1$, nach der gemachten Annahme existiert daher eine P nicht enthaltende Form Φ, so daß

$$f \cdot \Phi \equiv 0 \text{ mod. } (Q, u),$$

d. h.

$$\Phi \cdot f \equiv p \cdot u \text{ mod. } Q.$$

Es sei nun $f_1, \cdots, f_k$ eine Basis von Q_P; $\Phi_1, \cdots, \Phi_k$ seien wie oben Φ bestimmt. Es sei ferner $X = \Phi_1 \Phi_2 \cdots \Phi_k$ gesetzt. Dann ist

$$\begin{aligned} X \cdot f_1 &\equiv p_1 \cdot u \text{ mod. } Q, \\ X \cdot f_2 &\equiv p_2 \cdot u \text{ mod. } Q, \\ &\cdots\cdots\cdots \\ X \cdot f_k &\equiv p_k \cdot u \text{ mod. } Q. \end{aligned}$$

Nun gehören alle Formen von Q sicherlich zu Q_P. Somit ist

$$p_i \cdot u \equiv 0 \text{ mod. } Q_P.$$

Die Punkte des zu Q gehörigen Gebildes lassen sich nun mit Hilfe von $h-1$ Parametern analytisch darstellen. Sei s ein solcher Parameter

und für eine analytische Menge von Punkten P auf dem Gebilde von Q eine konvergente Potenzreihenentwicklung angesetzt

$$x_1 = s_1 = a_{1,1}\, s + a_{1,2}\, s^2 + \cdots$$
$$\cdots\cdots\cdots\cdots$$
$$x_{m-1} = s_{m-1} = a_{m-1,1}\, s + a_{m-1,2}\, s^2 + \cdots$$

Alsdann ist es möglich, die Noetherschen Bedingungen von M in einem Punkte $(s_1, \cdots, s_{m-1})$ bei unbestimmt bleibendem s zu berechnen. Man braucht ja nur, wenn $u_1, \cdots, u_h$ eine Basis von Q, $u_1, \cdots, u_h$ nach Potenzen von

$$x_1 - s_1 x_m,\ x_2 - s_2 x_m, \cdots, x_{m-1} - s_{m-1} x_m$$

zu entwickeln, dann, wie früher beschrieben, die $y_{n_1, \cdots, n_{m-1}}$ als lineare Formen von Unbestimmten zu entwickeln, und schließlich diese Unbestimmten nach der Reihe zu eliminieren. Durch einen rational ausführbaren Prozeß kann man also *alle* Noetherschen Bedingungen bis zu denen r^{ter} Ordnung finden, welchen die Formen von $Q_{(s_1, \cdots, s_{m-1})}$ genügen, wie groß auch r sei. Ist nun

$$\sum k \cdot \frac{\partial^j F(s_1, \cdots, s_{m-1})}{\partial x_1^{n_1}\, \partial x_2^{n_2} \cdots} + \cdots = 0$$

eine solche Noethersche Relation, die von jeder Form F von Q identisch befriedigt wird, so kann man sie im Bereiche ihrer Gültigkeit nach der Unbestimmten s beliebig oft differentiieren und erhält immer wieder von allen Formen von Q befriedigte Relationen, die Noethersche Bedingungen von $Q_{(s_1, \cdots, s_{m-1})}$ sein müssen. Dem vollständigen Systeme der Noetherschen Bedingungen von Q in $(s_1, \cdots, s_{m-1})$ gehören daher neben irgend einer $N(s) = 0$ auch alle $\frac{\partial^j N}{(\partial s)^j} = 0$ an. Genügt daher für ein bestimmtes $s = s_0 f$ den Noetherschen Bedingungen $Q_{(s_1, \cdots, s_{m-1})}$, so wird für ein unbestimmtes s in genügender Nähe von s_0,

$$s = s_0 + s',$$

da nach Taylor $N(s) = N(s_0) + \frac{dN(s_0)}{ds} \cdot s' + \cdots$, f *auch* die dazu gehörigen Noetherschen Bedingungen erfüllen.

Daraus folgt dann, daß es Punkte Q' in der Nachbarschaft von P gibt, so daß

$$Q_P = Q_{Q'}.$$

Es war aber

$$p_i \cdot u \equiv 0 \text{ mod. } Q_P,$$

somit ist auch

$$p_i \cdot u \equiv 0 \text{ mod. } Q_{Q'}.$$

u war eine beliebige Form, welche P enthält. Nach Bestimmung eines Q',

welches die oben geforderte Eigenschaft besitzt, bestimmen wir u so, daß es zwar P, aber nicht Q' enthält. Es folgt dann

$$p_i \equiv 0 \text{ mod. } Q_{Q'},$$

daher auch

$$p_i \equiv 0 \text{ mod. } Q_P.$$

Somit existieren Formen $a_{i,j}$, so daß

$$p_i = a_{i,1} f_1 + a_{i,2} f_2 + \cdots + a_{i,k} f_k.$$

Es ist also

$$\begin{aligned} X \cdot f_1 &\equiv (a_{1,1} f_1 + a_{1,2} f_2 + \cdots) u \text{ mod. } Q, \\ X \cdot f_2 &\equiv (a_{2,1} f_1 + a_{2,2} f_2 + \cdots) u \text{ mod. } Q, \\ &\cdots\cdots\cdots\cdots \\ X \cdot f_k &\equiv (a_{k,1} f_1 + \cdots) u \text{ mod. } Q, \end{aligned}$$

und daher, wenn

$$D = \begin{vmatrix} X - a_{1,1} u, & -a_{1,2} u, & \cdots \\ -a_{2,1} u, & X - a_{2,2} u, & \cdots \\ \cdots, & \cdots, & \cdots \end{vmatrix},$$

$$\begin{aligned} D \cdot f_1 &\equiv 0 \text{ mod. } Q, \\ D \cdot f_2 &\equiv 0 \text{ mod. } Q, \\ &\cdots\cdots \\ D \cdot f_k &\equiv 0 \text{ mod. } Q. \end{aligned}$$

Die Determinante D enthält P nicht, denn in P hat sie, da u in P gleich 0 ist, den Wert $(X)_P^k$ und X verschwindet nicht in P. D ist also relativ prim zu dem Gebilde von Q. Es folgt, da ja Q primär, $f_i \equiv 0$ mod. Q, d. h. jede Form von Q_P ist in Q enthalten. Auch das Umgekehrte ist der Fall. Folglich ist in der Tat $Q_P = Q$. Der aufgestellte Satz XXVII ist also ebenfalls erwiesen.

Es geht aus dem eben bewiesenen Satze hervor, daß die Bedingungen der Zugehörigkeit einer Form zu einem gegebenen Modul in die verschiedenste Gestalt gebracht werden können. Beispielsweise könnte man auf viele Arten eine endliche Zahl von Punkten $P_1, \cdots, P_j$ bestimmen, von der Eigenschaft, daß jede Form genügend hoher Ordnung, welche den Noetherschen Bedingungen von $M_{P_1}, \cdots, M_{P_j}$ genügt, notwendig in M enthalten sein muß.

45. Man kann von vorstehenden Sätzen eine sehr wichtige Anwendung auf die Theorie der Berührungen machen.

Um zunächst an einem besonderen Beispiele die der Anwendung zugrunde liegende Idee deutlich zu machen, betrachten wir ein System von $m - 1$ Formen

$$u_1, u_2, \cdots, u_{m-1},$$

deren Resultante mit einer unbestimmten Form nicht identisch verschwindet. Die Ordnungen der $u_1, \cdots, u_{m-1}$ seien $a_1, \cdots, a_{m-1}$.

Sind dann

$$P_1, P_2, \cdots, P_s$$

die verschiedenen Punkte des Schnitts von $u_1 = 0, \cdots, u_{m-1} = 0$, so läßt sich nach Satz XI setzen

$$(u_1, \cdots, u_{m-1}) = [Q_1, \cdots, Q_s],$$

wo nach Satz XXVII Q_i der zu P_i gehörige Noethersche Modul von

$$u_1, \cdots, u_{m-1}.$$

Nach Satz II ist die Anzahl der Bedingungen, die eine Form genügend hoher Ordnung befriedigen muß, um $(u_1, \cdots, u_{m-1})$ anzugehören,

$$= a_1 \cdots a_{m-1}.$$

Es ist leicht darzutun, daß die in den verschiedenen Q_i zum Ausdruck gebrachten Noetherschen Bedingungen für Formen genügend hoher Ordnung unabhängig voneinander sind. Somit ist als Gesamtzahl der zu den Q_i gehörigen Noetherschen Bedingungen $= a_1 \cdots a_{m-1}$. Nennen wir die Anzahl der Noetherschen Bedingungen von Q_i n_i, so ist also

$$n_1 + n_2 + \cdots + n_s = a_1 a_2 \cdots a_{m-1}.$$

Da nun die Zahl der $(m-1)$ Formen der Ordnungen $a_1, \cdots, a_{m-1}$ gemeinsamen Punkte im allgemeinen $a_1 \cdots a_{m-1}$ beträgt, so liegt es nahe, zu vermuten, daß, wenn die Zahl derselben, wie bei den Formen

$$u_1, \cdots, u_{m-1},$$

sich auf s reduziert, je n_i der Schnittpunkte im Punkte P_i koinzidieren.

Diese Vermutung bestätigt sich in der Tat, wie wir sehen werden.

Wir müssen zunächst präzisieren, was unter Koinzidenz zu verstehen ist.

Die Idee der Berührung entstand wohl zuerst am Kreise. Man hatte bewiesen, daß im allgemeinen eine Gerade zwei Punkte oder keinen Punkt mit ihm gemein habe, und fand dann als eine Art Übergang die Tangente. Ähnlich entstand die Idee der Koinzidenz an der quadratischen Gleichung. Zuerst war die Erkenntnis ihrer zwei Wurzeln, dann die *einer* Wurzel als Ausnahmefall, der durch Koinzidenz der beiden erklärt wurde. Bei jeder Anwendung des Begriffes der Koinzidenz oder Berührung muß man den historischen Werdeprozeß des Begriffes nachahmen, zunächst eine endliche Anzahl von Individuen als Funktion gewisser Unbestimmten definieren und dann nach den besonderen Werten der Unbestimmten fragen, für die durch stetigen Übergang mehrere der erwähnten Individuen ineinander fallen. Ohne Zuziehung von Unbestimmten haben die Begriffe Koinzidenz und Berührung keinen Sinn, und die durch dieselbe Konfiguration er-

zeugte Berührung oder Koinzidenz hat verschiedene Bedeutung, wenn verschiedene Gruppen von Unbestimmten den „allgemeinen" Fall ausdrückten.

In dem jetzt von uns zu untersuchenden Beispiel ist der „allgemeine" Fall der von $m-1$ Formen $f_1, \cdots, f_{m-1}$ der Ordnungen $a_1, \cdots, a_{m-1}$ mit lauter unbestimmten Koeffizienten. Ist

$$l = y_1 x_1 + \cdots + y_m x_m,$$

wo die $y_1, \cdots, y_m$ Unbestimmte, so ist die Resultante von $f_1, f_2, \cdots, f_{m-1}, l$ eine in lauter Linearfaktoren zerlegbare Form der y_i der Ordnung $r = a_1 \cdots a_{m-1}$:

$$\operatorname{Res}(f_1, f_2, \cdots, f_{m-1}, l) = L_1 L_2 \cdots L_r.$$

Diese Linearformen L_i seien die zu betrachtenden Individuen. Ist in dem besonderen Fall

$$f_1 = u_1, \cdots, f_{m-1} = u_{m-1}$$

die Resultante

$$= l_1^{c_1} l_2^{c_2} \cdots l_s^{c_s},$$

so können wir sagen, daß c_1 Koinzidenzen der L in l_1 stattfinden, c_2 in l_2 etc.; denn es ist klar, daß, wenn e eine beliebig kleine Größe und

$$f_1 = u_1 + e u_1', \cdots, f_{m-1} = u_{m-1} + e u_{m-1}',$$

wo die u_i' Formen mit unbestimmten Koeffizienten, die Linearfaktoren der Resultante von $(f_1, \cdots, f_{m-1}, l)$ für $\lim e = 0$ in die Linearformen $l_1, \cdots, l_s$ stetig übergehen.

Jedem der $l_1, l_2, \cdots, l_s$ entspricht einer der Punkte $P_1, P_2, \cdots, P_s$. Sei die Zuordnung der Linearformen l_i und Punkte P_i durch die Gleichheit des Index ausgedrückt. Unsere Behauptung ist dann äquivalent den Gleichungen

$$c_1 = n_1, c_2 = n_2, \cdots, c_s = n_s.$$

Die Ordnung der Resultante in den y_i ist

$$c_1 + c_2 + \cdots + c_s = n_1 + n_2 + \cdots + n_s.$$

Wir werden nun nachweisen, daß niemals sein kann $c_i < n_i$, welches auch der Index i sei. Die Behauptung wird damit evident sein.

Die Resultante R der

$$f_i = u_i + e \cdot u_i' \text{ und } l$$

ist ein Polynom der y_i, der Unbestimmten von u_i' und von e. Sind $L_1, \cdots, L_r$ die $a_1 \cdots a_{m-1}$ Linearformen, in welche R zerfällt, und ist p irgend ein Punkt des y-Raumes, so sind die $\frac{L_i}{(L_{i,p})}$ nach den Ausführungen des Kap. I Wurzeln einer Gleichung:

$$(p^r \times R) x^r - C_1 (p^{r-1} \times R) x^{r-1} + C_2 (p^{r-2} \times R) x^{r-2} - \cdots = 0,$$

wo die $C_1, \cdots, C_r$ numerische Konstante. x als Funktion von e betrachtet

ist daher algebraisch und hat bei $e = 0$ eine Verzweigung. Umgeben wir in einer komplexen e-Ebene den Nullpunkt mit einer beliebig kleinen Kontur und lassen diese sich zusammenziehen, so werden die entsprechenden x-Werte nach den Theorien von Puiseux sich in Gruppen von je $c_1, c_2, \cdots, c_s$ teilen, die für $\lim e = 0$ sich sämtlich beziehungsweise den Grenzwerten

$$\frac{l_1}{(l_{1,p})}, \frac{l_2}{(l_{2,p})}, \cdots, \frac{l_s}{(l_{s,p})}$$

nähern. Und zwar findet diese Annäherung in der Weise statt, daß eine rationale Potenz von e

$$y = e^{\frac{1}{\alpha}}$$

existiert, mit Hilfe deren die $a_1 \cdots a_{m-1}$ Zweige von x sich als konvergente Potenzreihen schreiben lassen

$$\frac{L_i}{(L_{i,p})} = \mathfrak{P}_i(y).$$

Betrachten wir nun folgende Menge von Formen

$$F = F_0 + e \cdot F_1 = p_1 (u_1 + e \cdot u_1') + p_2 \cdot (u_2 + e \cdot u_2') \\ + \cdots + p_{m-1} (u_{m-1} + e \cdot u_{m-1}'),$$

wo $p_1, p_2, \cdots, p_{m-1}$ Formen mit unbestimmten Koeffizienten. Eliminiert man diese Unbestimmten, indem man in obiger Beziehung die Koeffizienten von F als Veränderliche faßt, so kommt man auf ein System von Beziehungen, welche ausdrücken, daß F jeden der den L_i entsprechenden Punkte enthalte. Sieht man die $y_1, \cdots, y_m$ als zu den $x_1, \cdots, x_m$ kontragrediente Variable an, so ist jede dieser Beziehungen zu schreiben

$$(F \times L_i^r) = 0,$$

wo r die Ordnung von F.

Es gibt nun einen Satz, der hier von Diensten ist und der auch in anderen Disziplinen der Mathematik, z. B. der Theorie der Integrale linearer Differentialgleichungen, mit Erfolg verwendbar ist. Derselbe lautet:

Satz XXVIII: „Es seien $A_1, \cdots, A_n$ eine Reihe von Funktionen einer Anzahl Variabler und mögen die $A_1, \cdots, A_n$ auch von einem Parameter y analytisch-regulär abhängen. Es seien ferner für unbestimmte Werte von y die $A_1, \cdots, A_n$ durch eine Reihe linear-independenter Beziehungen verknüpft, deren Anzahl k ist:

$$\text{(R)} \qquad \begin{aligned} a_{1,1} A_1 + \cdots + a_{1,n} A_n &= 0, \\ a_{2,1} A_1 + \cdots + a_{2,n} A_n &= 0, \\ \cdots\cdots\cdots\cdots \\ a_{k,1} A_1 + \cdots + a_{k,n} A_n &= 0, \end{aligned}$$

die $a_{i,j}$ als analytisch reguläre Funktionen von y, in bezug auf die Variablen aber als Konstante verstanden. Alsdann läßt sich immer durch rein rationale Operationen den Relationen (R) eine Gestalt geben, daß für irgend einen *bestimmten* Wert von y aus ihnen k linear-unabhängige Relationen folgen."

Zur Erläuterung sei hinzugefügt, daß der erwähnte bestimmte Wert von y dem Konvergenzbereich der A_i wie $a_{i,k}$ angehören muß.

Sei der Einfachheit halber der in Frage kommende Wert von y die Null. Von den Relationen (R) können und wollen wir voraussetzen, daß sie „reduziert" sind, d. h. daß keiner der Ausdrücke $A_1, \cdots, A_n$ durch eine Potenz von y teilbar sei, noch daß die $a_{i,1}, \cdots, a_{i,n}$ für irgend einen Index i eine Potenz von y als gemeinsamen Teiler enthalten. Wenn für $y = 0$ die Relationen (R) linear-unabhängig bleiben, so ist es nicht erst nötig, dieselben zu verändern, um das gewünschte Resultat zu erzielen. Ist dies jedoch nicht der Fall, so muß jedenfalls jede k-gliedrige Determinante der Matrix

$$\Delta = \begin{vmatrix} a_{1,1} & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & a_{k,n} \end{vmatrix}$$

für $y = 0$ verschwinden. In diesem Falle gibt es eine Zahl l, so daß alle Determinanten von Δ durch y^l, doch nicht durch y^{l+1} teilbar sind, da ja die $a_{i,k}$ nach Voraussetzung in konvergente Potenzreihen von y entwickelbar sind. Auch gibt es von Null verschiedene Zahlen $z_1, \cdots, z_k$, so daß gleichzeitig

$$\begin{aligned} b_1 &= a_{1,1}z_1 + a_{2,1}z_2 + \cdots + a_{k,1}z_k = 0, \\ b_2 &= a_{1,2}z_1 + a_{2,2}z_2 + \cdots + a_{k,2}z_k = 0, \\ &\cdots\cdots\cdots\cdots\cdots \\ b_n &= a_{1,n}z_1 + a_{2,n}z_2 + \cdots + a_{k,n}z_k = 0, \end{aligned}$$

wenn $y = 0$. Mithin ist für die erwähnten Zahlen z_i jede der obigen Funktionen von y durch eine Potenz von y, sagen wir mindestens y^l, teilbar. Es habe eine der von 0 verschiedenen Zahlen z den Index k. Ersetzt man dann (R) durch das ihm äquivalente System, welches aus (R) entsteht, indem für die Reihe $a_{k,1}A_1 + \cdots + a_{k,n}A_n = 0$ die andere $b_1A_1 + \cdots + b_nA_n = 0$ tritt, so ist nun das System nicht mehr „reduziert", Es sei $b_i = y^l c_i$ und sei das System von Relationen (R) jetzt geschrieben

$$(\mathrm{R}') \qquad \begin{aligned} a_{1,1}A_1 + \cdots + a_{1,n}A_n &= 0, \\ \cdots\cdots\cdots\cdots \\ a_{k-1,1}A_n + \cdots + a_{k-1,n}A_n &= 0, \\ c_1A_1 + \cdots + c_nA_n &= 0. \end{aligned}$$

(R′) ist dann (R) für jeden Wert von y äquivalent, und jede der Determinanten der zu (R′) gehörigen Matrix ist durch eine um l' kleinere Potenz von y als die entsprechende Determinante der zu (R) gehörigen Matrix teilbar. Ist nun (R′) nach Einsetzung von $y = 0$ noch immer kein linear-unabhängiges System, so wiederhole man den eben beschriebenen Prozeß. Da l eine positive ganze Zahl, so muß nach einer endlichen Zahl von Ausführungen des erwähnten Prozesses schließlich ein (R) für alle Werte von y äquivalentes System von Relationen erhalten werden, welches auch für $y = 0$ noch k linear-unabhängige Beziehungen zwischen den $A_1, \cdots, A_n$ liefert, und die Behauptung ist damit verifiziert.

Dabei ist noch ersichtlich, daß bei Ausführung des Prozesses nur eine endliche Zahl der Koeffizienten der Reihenentwicklung der $a_{i,j}$ in Betracht kommen.

Betrachten wir nun das System der Relationen

$$\text{(R)} \qquad (F \times L_i^r) = 0,$$

welche F befriedigt. Für $\lim e = 0$ fallen die L_i in verschiedenen Punkten zusammen, und das System (R) hört auf, so viel verschiedene Aussagen zu enthalten als für unbestimmte e. Wenden wir aber den Prozeß an, welcher eben geschildert war, so erhalten wir in jedem Punkte P_i genau c_i linearunabhängige Relationen der Gestalt

$$\begin{gathered}(F \times A_i) = 0,\\ (F \times B_i) = 0,\\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\end{gathered}$$

welche auch noch linearunabhängig bleiben, wenn $y = 0$ gesetzt wird. Zudem ist klar, daß bei Ausübung des Prozesses nur eine endliche Anzahl der Glieder der Entwicklung von $(F \times L_i^r)$ nach Potenzen von y in Betracht kommen. Die Entwicklung von $(F \times L_i^r)$ geschieht nach dem Theorem von Taylor, die Koeffizienten dieser Entwicklung sind also Differentialausdrücke von F in einem der Punkte P_i, und jeder der

$$(F \times A_i) = 0,\ (F \times B_i) = 0,\ \cdots$$

ist demnach in $y = 0$ nur ein anderer Ausdruck für eine Noethersche Bedingung bei P_i. Der Ausdruck F genügt somit in jedem der Punkte P_i, wenn $e = 0$ ist, zum mindesten den c_i Bedingungen, die durch den Grenzübergang

$$\lim y = 0$$

aus $(F \times A_i) = 0$, $(F \times B_i) = 0$, $\cdots$ entstehen. Daher ist $n_i \geqq c_i$.

Nach den übrigen Voraussetzungen war aber

$$\sum n_i = \sum c_i,$$

mithin ist notwendigerweise $n_i = c_i$. Q. e. d.

46. Genau derselbe Gedankengang führt auch dann noch zum Ziel, wenn die Voraussetzungen des allgemeinen Falles andere sind.

Sei eine Anzahl von Primmoduln

$$P_1, \cdots, P_j$$

so gegeben, daß die Summe ihrer Stufen $m-1$ betrage. Seien die zugehörigen irreduziblen Gebilde $C_1, \cdots, C_j$, seien dieselben von Unbestimmten abhängig, und mögen die $C_1, \cdots, C_j$ eine Anzahl N von Punkten gemein haben, die von den Unbestimmten unabhängig sei. Es sei schließlich die Hilbertsche Funktion von $(P_1, \cdots, P_j) = N$. Alsdann wird die Zahl der Berührungen von $C_1, \cdots, C_j$ für spezielle Werte der Unbestimmten in irgend einem Punkte P durch die Zahl der Noetherschen Bedingungen des entsprechenden Moduls $(P_1, \cdots, P_j)$ in P gemessen.

Ist überhaupt M ein Modul, der selbst von Unbestimmten abhängt, dessen Hilbertsche Funktion aber von diesen Unbestimmten unabhängig ist; besteht ferner das Gebilde von M aus lauter Punkten $P_1, P_2, \cdots, P_j$ und hat M_{P_i} die Hilbertsche Funktion n_i, so wird durch Verschmelzung von zweien oder mehreren der P_i die Summe $\sum n_i$ erstreckt über die koinzidierenden Punkte nicht geändert. Eine Anwendung dieser Sätze liegt in der Berechnung der Zahl der Koinzidenzen in einem Punkte A von $m-1$ Formen $u_1, \cdots, u_{m-1}$, welche A resp. zu einem $a_1, \cdots, a_{m-1}$-fachen Punkt besitzen. Wir nehmen als Entwicklung bei A an

$$u_i = \sum u_{i,j},$$

wo $u_{i,j}$ A als j-fachen Punkt enthält. Ferner setzen wir voraus, daß die Resultante der Anfangsterme

$$u_{1,a_1}, \cdots, u_{m-1,a_{m-1}},$$

die ja Formen in nur $m-1$ Variablen sind, nicht verschwindet. Alsdann ist die Zahl der Noetherschen Bedingungen, also die der Koinzidenzen, von $(u_1, \cdots, u_{m-1})_A$ gleich

$$a_1 a_2 \cdots a_{m-1}.$$

Betrachtet man nämlich

$$(u_1, \cdots, u_{m-1})_A$$

als P-Modul bei A und untersucht den entsprechenden (früher M' genannten) Modul, so findet man bei Anwendung der früher benutzten Schlußreihe, daß hier nicht bloß die Beziehung $H(u_1, \cdots, u_{m-1})_A = HM'$ für große Werte der Ordnung sich ergibt, sondern wegen Satz I für *alle* Werte der Ordnung. Danach ist die Zahl aller Noetherschen Bedingungen von $(u_1, \cdots, u_{m-1})_A$ gleich

$$\text{(R)} \qquad \sum H(u_{1,a_1}, \cdots, u_{m-1,a_{m-1}}) R,$$

die Summe ausgedehnt über *alle* Ordnungen R von $R=1$ an. Es ist

nicht schwer, diese Summe nach Satz II zu berechnen, doch genügt ja schon der Hinweis, daß nach Satz II die Anzahl der Noetherschen Bedingungen von $u_{1,a_1}, \cdots, u_{m-1,a_{m-1}}$, als Formen von m Variablen aufgefaßt, $= a_1 \cdots a_{m-1}$ sein muß, während diese Formen doch keinen anderen Punkt als A gemeinsam haben.

Für Werte von

$$R > a_1 + a_2 + \cdots + a_{m-1} - m + 1$$

ist $H(u_{1,a_1}, \cdots, u_{m-1,a_{m-1}})$ im Bereiche von $m-1$ Variablen gleich Null, nach Satz II. Somit sind die Noetherschen Bedingungen von

$$(u_1, \cdots, u_{m-1})_A$$

von höchstens der Ordnung $a_1 + \cdots + a_{m-1} - m + 1$.

All dies gilt auch, wenn $u_1, \cdots, u_{m-1}$ analytische Funktionen bei A sind.

Kapitel IV.

Erweiterung auf Formen von mehreren Reihen von Variablen.

47. Der Raum $x_1, \cdots, x_m$ war bisher der einzige, in dem alle Operationen gedeutet waren. Es ist aber naturgemäß bei Aufgaben mancherlei Art, mehrere Räume einzuführen. Wollten wir z. B. eine Theorie der Konkomitanten eines Systems von Formen bestimmter Ordnungen

$$f_1, f_2, \cdots, f_h$$

schreiben, so müßten wir die Koeffizienten der Formen $f_1, \cdots, f_h$ als Unbestimmte auffassen, und jene Konkomitanten als Formen dieser Unbestimmten deuten. Der Komplex der Koeffizienten jeder einzelnen der Formen würde dann ein schon in sich abgerundetes Etwas, ein Raum, sein. Schon aus diesem Grunde ist es in der Algebra unerläßlich, den Betrachtungen eine Gruppe von Räumen

$$\begin{array}{c} x_{1,1}, \cdots, x_{1,m_1}, \\ x_{2,1}, \cdots, x_{2,m_2}, \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ x_{k,1}, \cdots, x_{k,m_k} \end{array}$$

zugrunde zu legen.

Die Anzahl dieser Räume braucht keine endliche zu sein, wenn Grenzübergänge aus unseren algebraischen Untersuchungen nicht ausgeschlossen sind. Wir werden uns jedoch auf eine endliche, wenn auch unbestimmte Anzahl von Räumen beschränken.

Der Raum $x_{i,1}, \cdots, x_{i,m_i}$ heiße S_i, die Gruppe der Räume $S_1, \cdots, S_k$ sei kurz S, und die Summe

$$(m_1 - 1) + (m_2 - 1) + \cdots + (m_k - 1) = m - 1$$

heiße die Dimension von S. Die Algebra der Formen in S heiße die „Algebra in S".

Eine Form in S, welche in bezug auf die Variablen jeder der S_i homogen von der Ordnung n_i ist, heißt eine Form der Ordnungen

$$n_1, n_2, \cdots, n_k.$$

Enthält eine Form die Variablen eines Raumes gar nicht, so ist natürlich die Ordnungszahl der Form in bezug auf den betreffenden Raum $= 0$.

Die Anzahl der Koeffizienten einer Form der Ordnungen $n_1, \cdots, n_k$ wird mit

$$\varphi(n_1, \cdots, n_k)$$

bezeichnet. Dieselbe ist

$$\varphi(n_1, \cdots, n_k) = \varphi_1(n_1) \cdot \varphi_2(n_2) \cdots \varphi_k(n_k),$$

wenn φ_i die φ-Funktion des Raumes S_i bedeutet. Dies Theorem ist durch eine sehr einfache Abzählung erweisbar.

Ein System von Punkten $P_1, \cdots, P_k$ in $S_1, \cdots, S_k$ resp. sei ein Element von S. m Formen in S mit unbestimmten Koeffizienten haben kein Element gemein, wie sich nach der im Kap. I angewandten Überlegung sogleich ergibt. $m - 1$ Formen in S mit unbestimmten Koeffizienten dagegen haben „im allgemeinen", welcher Ausdruck später präzisiert werden wird, eine endliche Anzahl von Elementen gemein, und daher gibt es, wenn m Formen in S mit unbestimmten Koeffizienten vorliegen, im allgemeinen eine Form dieser Unbestimmten, deren Verschwinden die notwendige und hinreichende Bedingung für die Existenz eines den Formen gemeinsamen Elementes ist. Daß, wenn diese Form existiert, dieselbe irreduzibel ist, zeigt sich nach den Überlegungen des Kap. I. Auch ist ersichtlich, nach derselben Schlußreihe, daß, wenn $l_1, l_2, \cdots, l_k$ Linearformen in $S_1, \cdots, S_k$, $f_1, \cdots, f_m$ die m Formen in S, R die eben charakterisierte Form der Unbestimmten, Zahlen $M_1, \cdots, M_k$ existieren, so daß

$$R \cdot l_1^{M_1} \cdots l_k^{M_k} = p_1 f_1 + \cdots + p_m f_m,$$

wo $p_1, \cdots, p_m$ ganzzahlige Formen in S und der Unbestimmten von

$$f_1, \cdots, f_m.$$

Die soeben charakterisierte Form R sei „Resultante in S" von $f_1, \cdots, f_m$ genannt. Sie existiert nur dann nicht, wenn, entgegen den Voraussetzungen der im Kap. I gemachten Schlüsse, $m - 1$ der Formen f_i kein gemeinsames Element haben, was nur zutreffen kann, wenn weniger als $m_i - 1$ der Formen f_j eine von 0 verschiedene Ordnung n_i in S_i haben.

Haben genau $m_i - 1$ der Formen f_j eine von 0 verschiedene Ordnung n_i in S_i, so treten diese Formen sowohl wie S_i aus der Betrachtung, und die „Resultante in S" von $f_1, \cdots, f_m$ reduziert sich auf die „Resultante in S'" von denjenigen Formen $f_1, \cdots, f_m$, die von den Variablen S_i unabhängig sind, wobei S' die Gruppe $S_1, \cdots, S_k$ mit Ausschluß von S_i bezeichnet. Wird die Resultante in S von $f_1, \cdots, f_m$ mit $R(f_1, \cdots, f_m)$ bezeichnet, so ist identisch

$$R(f_1, f_2, \cdots, f_{m-1}, g \cdot h) = R(f_1, \cdots, f_{m-1}, g) \cdot R(f_1, \cdots, f_{m-1}, h),$$

wie sich nach den Schlüssen des Kap. I ergibt.

Die Schlüsse des Satzes IV ergeben in S die Existenz „irreduzibler Bildungen" und die eindeutige Zerlegung von „Konfigurationen" in selben. Dabei ist nur, wegen des Vorhandenseins des Ausnahmefalles, festzuhalten, daß Formen, die keine Resultante besitzen, niemals gemeinsame Elemente haben können.

Ein „irreduzibles Gebilde" in S wollen wir eine irreduzible „Korrespondenz" oder „Verwandtschaft" nennen. Denn das entspricht genau dem gewöhnlichen Sprachgebrauch der Mathematiker. Die Stufe der Korrespondenz oder Verwandtschaft ist dann ein der Stufe eines irreduziblen Gebildes, wie es ursprünglich verstanden war, analoger Begriff. Ebenso werden wir von der Mannigfaltigkeit oder Dimension einer Verwandtschaft sprechen, als der Mannigfaltigkeit resp. Dimension des Systems von Elementen, welche den Bedingungen der Verwandtschaft entsprechen. Beispielsweise, wenn die Punkte zweier Kurven A, B, die resp. in den Räumen A', B' gelegen sind, durch die Verwandtschaft V einander eindeutig zugeordnet sind, wird V die Mannigfaltigkeit 2, die Dimension 1 haben. Ist dagegen jeder Punkt von A jedem Punkt von B zugeordnet, so haben wir es mit einer Korrespondenz der beiden Räume A', B' der Dimension 2 zu tun. Oder haben wir es mit einer Verwandtschaft V zu tun, welche in drei Räumen A', B', C', Punkten eines Gebildes A der Mannigfaltigkeit 4 je ein bestimmtes Punktepaar zweier Gebilde B, C zugeordnet, so hat V die Mannigfaltigkeit 4 und Dimension 3 etc. etc.

48. Es ist klar, daß die Gesamtheit der in S existierenden Formen, welche in den Elementen einer irreduziblen Verwandtschaft V verschwinden, einen Primmodul bilden, wie überhaupt die Definitionen und Sätze des Kap. II ohne weiteres auch für die Algebra in S existenzfähig bleiben. Nur die Begriffe und Sätze des Kap. I und III bedürfen für die hier zugrunde liegende Algebra in manchen Punkten einiger Modifikationen und Erläuterungen.

Der Satz I (Kap. I) z. B. hört auf, in der früher angegebenen Gestalt richtig zu sein. Es ist nötig, eine beschränkende Bedingung hinzuzu-

fügen. Er lautet für die Algebra in S: „Sind $u_1, \cdots, u_h$ $(h \leqq m)$ Formen in S, deren Resultante mit $m-h$ beliebig zu wählenden Formen nicht identisch verschwindet, besteht eine identische Beziehung

$$p_1 u_1 + \cdots + p_h u_h = 0$$

und sind die Ordnungen von jedem der p_i mindestens gleich den entsprechenden Ordnungen irgend eines der u_j (mit Ausschluß von u_i), so gibt es Formen $q_{i,j}$, für welche identisch

$$q_{i,j} + q_{j,i} = 0, \quad p_i = \sum q_{i,j} u_i, \quad q_{i,i} = 0."$$

Eine die Ordnungen der p_i beschränkende Bedingung irgend einer Art ist notwendig, denn, wie schon das Beispiel der Resultante zeigt, Beziehungen der diskutierten Gestalt bestehen wirklich, ohne daß die Formen $q_{i,j}$ existieren. Daß die angegebene Bedingung genügend ist, ergibt sich leicht bei Betrachtung des Induktionsbeweises von Satz I. Die betreffende Bedingung ist sowohl notwendig wie hinreichend, wenn der Raum S_i aus einer einzigen Variablen besteht, auf diesen Fall führt aber der Induktionsbeweis den Satz zurück. Nur *ein* Schluß der ganzen Schlußreihe des Beweises wird infolge der zugefügten Bedingung ungültig. Nachdem nämlich für $h = m$ erwiesen war, daß, wenn

$$p_1 u_1 + \cdots + p_h u_h = 0$$

und die Resultante von $u_1, \cdots, u_h$ mit $m-h$ beliebigen Formen nicht verschwindet, Formen $q_2, \cdots, q_h$ existieren, für die

$$p_1 = q_2 u_2 + \cdots + q_h u_h,$$

erschlossen wir die Gültigkeit des obigen für $h < m$ einfach durch Adjunktion von Formen $u_{h+1}, \cdots, u_m$, deren Ordnung größer war als die jedes der p_i. Dies Verfahren versagt hier infolge der Beschränkung für die Ordnungen der p_i. Die so entstandene Lücke im Beweis füllen wir in folgender Weise aus.

Das befolgte Beweisverfahren macht zunächst klar, daß, wenn der behauptete Satz richtig ist für einen Raum S der Mannigfaltigkeit $m-1$, aus einer Beziehung der Gestalt

$$p_1 u_1 + \cdots + p_{h-1} u_{h-1} + p_h \cdot l = 0,$$

wo l linear ist, und die übrigen Voraussetzungen des Satzes erfüllt sind, immer folgt $p_h = q_1 u_1 + \cdots + q_{h-1} u_{h-1}$. Dies gilt für jeden Wert von h. Ist nun $h < m$, also $h - 1 < m - 1$, so kann man 2 Linearformen bestimmen, deren Resultante mit $u_1, \cdots, u_{h-1}$ und $m-h-1$ beliebig zu wählenden Formen nicht verschwindet. Diese beiden seien der Einfachheit halber mit x_1 und x_2 identisch. Alsdann definiere ich eine Größe y durch die Beziehung $x_2 = y \cdot x_1$ und betrachte die Identität

$$p_1 u_1 + \cdots + p_h \cdot u_h = 0$$

als eine solche für einen Raum der Mannigfaltigkeit $m-1$, indem in ihr überall $x_2 = y \cdot x_1$ gesetzt und y als Parameter angesehen wird. Es folgt, nach Voraussetzung, wenn $(U_i)_{x_2=yx_1}$ noch mit U_i bezeichnet wird, $p_h = r_1 U_1 + \cdots + r_{h-1} U_{h-1}$, wo die $r_1, \cdot \cdot, r_{h-1}$ von y rational abhängen, also $p_h \cdot Y = s_1 U_1 + \cdots + s_{h-1} U_{h-1}$, wo $s_1, \cdots, s_{h-1}$ Formen der Variablen und Polynome von y, Y nur von y abhängig ist. Ersetze ich in dieser Beziehung wieder y durch $\frac{x_2}{x_1}$ und mache die resultierende Identität homogen, so zeigt sich

$$p_h \cdot Z = t_1 u_1 + \cdots + t_{h-1} u_{h-1},$$

wo Z eine Form von x_1 und x_2 ist und die t_i Formen in S sind. Z ist als binäre Form darstellbar als Produkt von Linearformen der Gestalt $ax_1 + bx_2$, wo a, b Konstante. Somit ergibt sich, da nach Voraussetzung die Resultante irgend einer dieser Linearformen, von $u_1, \cdots, u_{h-1}$ und $m-h$ beliebig zu wählenden Formen nicht identisch verschwindet, durch sukzessive Anwendung des früher hier für die Beziehung

$$p_1 u_1 + \cdots + p_h \cdot l = 0$$

erhaltenen Resultates,

$$p_h = q_1 u_1 + \cdots + q_{h-1} u_{h-1}.$$

Damit ist Satz I auch für die Algebra in S vollständig erwiesen.

49. Führen wir nun in Analogie zum ersten Kapitel ein Operationssymbol

$$\Delta_{n_1, n_2, \cdots, n_k}$$

ein, es durch die Beziehung

$$\Delta_{n_1, \cdots, n_k} f(r_1, \cdots, r_k) = f(r_1, \cdots, r_k) - f(r_1 - n_1, \cdots, r_k - n_k)$$

definierend, so können wir auch in S den Sätzen II und III des ersten Kapitels genau analoge Sätze aufstellen. Sind

$$(n_{1,1}, \cdots, n_{1,k}), \cdots, (n_{h,1}, \cdots, n_{h,k})$$

die Ordnungen von $u_1, \cdots, u_h$, so ist

$$H(u_1, \cdots, u_h)(R_1, \cdots, R_k) = \Delta_{n_{1,1}, \cdots, n_{1,k}} \cdots \Delta_{n_{h,1}, \cdots, n_{h,k}}(r_1, \cdots, r_k),$$

wenn

$$R_i > n_{i,1} + n_{i,2} + \cdots + n_{i,h} - m_i;$$

dagegen um 1 mehr oder minder, wenn alle

$$R_i = n_{i,1} + n_{i,2} + \cdots + n_{i,h} - m_i.$$

Was geschieht, wenn einzelne der R_i größer, andere kleiner sind als die angegebenen Werte, bleibt danach noch unentschieden. Diese Frage scheint überhaupt eine schwierige und kaum mit den bisher verwandten Mitteln lösbar zu sein. Da sie zudem zu all den Anwendungen, welche in den Schlußbemerkungen besprochen sind, in nur ganz loser Be-

ziehung steht, so ist ein Eingehen auf diese Frage an dieser Stelle noch nicht nötig.

Die Existenz der Form Ω bleibt nach obigem ungeschmälert erhalten; auch der Satz, daß nur die Formen f apolar zu $\Omega(u_1, \cdots, u_m)$ dem Modul $(u_1, \cdots, u_m)$ angehören, unter f Formen verstanden, deren Ordnungen kleiner oder höchstens gleich denen von Ω sind.

Die Betrachtungen des Satzes IV und des Kap. II bleiben in Kraft. Doch bedarf Satz XI der Einschränkung, daß, wenn $C_1, \cdots, C_a$ die irreduziblen Gebilde, in die $u_1, \cdots, u_h$ zerfällt, und $M = (u_1, \cdots, u_h)$, dann $M = [M_{C_1}, \cdots, M_{C_a}, r]$, wo der Modul r alle die Formen enthält, deren Ordnungen in jedem der S_i diejenigen jedes der u_i mindestens erreichen. Es ist dies eine offenbare Folge der in der Algebra in S beim Analogon zu Satz I zu machenden Einschränkung.

Die Definition der Hilbertschen Funktion des Moduls M als einer von den k Ordnungen der Funktion abhängigen Zahl bleibt ungeändert. Nur lautet Satz IX in der Algebra in S: „Die Hilbertsche Funktion eines Moduls M

$$HM(r_1, \cdots, r_k)$$

ist für genügend große Werte von $r_1, r_2, \cdots, r_k$ ein Polynom von $r_1, \cdots, r_k$, dessen Ordnung um 1 kleiner ist als die Mannigfaltigkeit von M, und in irgend einer ausgewählten Gruppe der $r_1, \cdots, r_k$, etwa $r_{i_1}, r_{i_2}, \cdots, r_{i_h}$, nur zu der Ordnung ansteigt, welche der Mannigfaltigkeit von Elementen entspricht, die der Modul M in den korrespondierenden Räumen $S_{i_1}, \cdots, S_{i_h}$ besitzt."

Der Beweis dieses Satzes geht im übrigen nach demselben Prinzip vor sich wie derjenige des Satzes IX.

Wir kommen nun zur Frage, was in der Algebra in S unter den Noetherschen Bedingungen eines Moduls zu verstehen sei und inwieweit in ihr die Betrachtungen des Kap. III gültig bleiben.

Statt des Punktes P des Kap. III werden wir Element, statt der Ordnung r Ordnungen $r_1, \cdots, r_k$ sagen müssen, doch bleiben alle Erwägungen bestehen, bis zur Einführung des dem analytischen P-Modul M entsprechenden Modul M'. Nur dann wird die Form p dem Modul M' angehören dürfen, wenn ein Individuum von M eine Entwicklung hat

$$f = p + p' + p'' + \cdots,$$

welche p enthält, und zwar so, daß die Ordnungen der übrigen Terme zum mindesten in einem der Räume S_i größer sind als die Ordnungen von p, in keinem der Räume S_i aber kleiner. Offenbar folgt dann für die Noether-Hilbertsche Funktion von M'

$$(N, H)\, M(r_1, r_2, \cdots, r_k) = HM'(r_1, r_2, \cdots, r_k),$$

genau so wie in Kap. III.

Alle übrigen Folgerungen bleiben unverändert. Analoge Bemerkungen muß man über die Ideale in S machen.

50. Zum Schluß möchte ich noch bemerken, daß man unschwer die aufgestellten Sätze nach verschiedener Richtung hin erweitern könnte. Einige Erweiterungen der Theorie der Elementarteiler sind bekannt. Genau dieselben Erweiterungen sind möglich bei der Definition und den Sätzen über die Ideale. Die Ausführungen des Kap. III sind übertragbar auf Formen, deren Koeffizienten ganze Zahlen sein oder einem bestimmten Körper angehören sollen. Denn Satz XXIII, und damit auch alle anderen Sätze bleiben auch bei dieser Einschränkung erhalten. Man kann Kap. III erweitern, indem man den Punkt P ersetzt durch ein Primideal J m^{ter} Stufe und, nach dem Vorbilde der Methoden von Hensel, Entwicklungen nicht bloß nach Variablen, sondern auch nach Potenzen der in J enthaltenen Primzahl p betrachtet. Man kann auch die Schlüsse ausdehnen auf die Menge der analytischen Funktionen, welche in einem gegebenen Bereich B keine Singularitäten haben. Neue Schwierigkeiten sind bei diesen Erweiterungen kaum zu überwinden.

Schlußbemerkungen über einige Anwendungen der aufgestellten Sätze.

51. Es war ursprünglich meine Absicht, den Ausführungen der vorgehenden Kapitel einige Anwendungen beizufügen, doch ist der Stoff schon zu stark angewachsen. Zudem kann es nicht die Aufgabe desjenigen, der neue Resultate bieten will, sein, sie sofort im ganzen Umfange ihrer Bedeutung anzuwenden. Daher entschloß ich mich, wiewohl schwer, auf das Kapitel der Anwendungen zu verzichten. Doch glaube ich, die hauptsächlichsten der Zielpunkte, die mir außer dem rein theoretischen der Erweiterung des Noetherschen Theorems noch vorschwebten, kurz andeuten zu sollen, sei es auch nur, um die Arbeit verständlicher zu machen.

Zu alleroberst würde da ein Satz stehen, der einen Fundamentalsatz der Lehre von den Verwandtschaften mit umfaßt. Drückt man die Hilbertsche Funktion eines Moduls M mit Hilfe von Differenzensymbolen, welche in bezug auf die φ-Funktion gemeint sind, gemäß der Gleichung $HM(r_1, \cdots, r_k) = H' \varphi(r_1, \cdots, r_k)$ aus, so ist das Differenzensymbol H' eindeutig bestimmt. Der Operator H' sei der „Hilbertsche Operator des Moduls M“ genannt. Nennt man nun zwei primäre Moduln A und B der Stufen a und b relativ prim, wenn (A, B) die Stufe $a + b$ hat, und irgend zwei Moduln relativ prim, wenn alle ihre primären Teiler relativ prim zueinander sind, so gilt der Satz, daß der Hilbertsche Operator

des größten Teilers zweier relativ primer Moduln das Produkt der Hilbertschen Operatoren der beiden Moduln ist. Ein Weg zum Beweis des Satzes ist der folgende. Zunächst zeige man, daß, wenn A, B zwei relativ prime Moduln sind, und $a_1, \cdots, a_h$ eine Basis von A, $b_1, \cdots, b_k$ eine solche von B ist, dann für genügend hohe Ordnungen $(a_1 \cdot b_1, \cdots, a_h \cdot b_k)$ eine solche von $[A, B]$ ist. Danach erweitere man diesen Satz auf das System der Syzygien eines der Moduln z. B. A, und zeige, daß unter der Voraussetzung, daß A und B relativ prim sind, die Kongruenz

$$X_1 a_1 + \cdots + X_h a_h \equiv 0 \text{ mod. } B$$

und die aus ihr folgenden syzygetischen Kongruenzen modulo B die Kette der Syzygien von A erzeugt, wenn man sich auf genügend hohe Ordnungen beschränkt. Alsdann berechne man die Konstantenzahl von Formen gegebener Ordnungen von (A, B) auf dem Wege, wie Hilbert im Beweise seines Theorems IV die Konstantenzahl der Formen gegebener Ordnungen von A berechnet.

Eine spezielle Anwendung des obigen Satzes ist folgende. Sind $A, B, \cdots, L$ eine Reihe von irreduziblen Korrespondenzen, $A, \cdots, L$ die entsprechenden Primmoduln, und ist die Summe der Stufen $a + b + \cdots + l$ von $A, \cdots, L$ gleich $m - 1$, so haben $A, B, \cdots, L$ immer dann, und nur dann, eine endliche Zahl gemeinsamer Elemente, wenn $A, B, \cdots, L$ relativ prim zueinander sind, und die Zahl dieser gemeinsamen Elemente ist

$$\alpha \beta \cdots \lambda \; \varphi(R_1, \cdots, R_k),$$

wo $\alpha, \cdots, \lambda$ die Hilbertschen Operatoren von $A, \cdots, L$ sind.

Man kann aus den Anwendungen dieser Formel ersehen, daß die Symbole des Bedingungskalkuls von Schubert als Hilbertsche Operatoren interpretiert werden können und in dieser Auffassung alles Hypothetische verlieren.

52. Eine andere Anwendung unserer Ergebnisse betrifft diejenigen Probleme, welche zuerst von den englischen Mathematikern Cayley, Salmon u. a. behandelt und von letzterem unter dem Titel „Order of restricted systems of equations“ bekannt gemacht wurden.*) Das Problem, wie es von den genannten Mathematikern gestellt wurde, ist folgendes. Eine Zahl von $m - 1$ Formen haben eine Reihe von Gebilden, Kurven, Oberflächen etc. gemein. Wieviel Punkte haben sie noch gemein, welche nicht auf jenen Kurven, Oberflächen etc. liegen? Diese Frage suchte Salmon zu beantworden, und fand die im wesentlichen richtige Lösung, obwohl ihm nur ganz unzulängliche Hilfsmittel zu Gebote standen. Für uns ist der Satz VII mit den verwandten Sätzen ein Stützpunkt, der

*) Lessons on Modern Higher Algebra.

uns erlaubt, nicht bloß das Problem richtig zu stellen, sondern auch einen Weg zur Lösung einzuschlagen.

Wir werden die gegebenen Kurven, Oberflächen etc. und die Art ihrer gegenseitigen Lage, wie auch die Art, in der die gegebenen Formen dieselben enthalten sollen, dadurch ausdrücken können, daß wir sagen, die gegebenen $m-1$ Formen $f_1, \cdots, f_{m-1}$ gehören einem bestimmten Modul M an. Das Salmonsche Problem richtet sich dann auf die Hilbertsche Funktion desjenigen Teilers von

$$(f_1, \cdots, f_{m-1}),$$

der sich nicht auf die Gebilde von M bezieht. Durch die Diskussion der Gleichung

$$X_1 f_1 + \cdots + X_h f_h = 0$$

für unbestimmte Formen f_i des Moduls M, wobei

$$h \leqq m,$$

zeigt sich dann, daß die den $f_1, \cdots, f_{h-1}$ gemeinsamen Gebilde, die nicht auf denen von M liegen, Hilbertsche Operatoren besitzen, die von den Ordnungen der f_i rational und ganz abhängen, aber sonst von den unbestimmten Koeffizienten der f_i unabhängig sind. Auf dieser Grundlage ergibt sich z. B. das folgende Resultat: Es sei C eine irreduzible Verwandtschaft, $A_1, \cdots, A_n$ seien n irreduzible Verwandtschaften der Stufen $a_1, \cdots, a_n$ und mögen die $A_1, \cdots, A_n$ sämtlich C enthalten. Ferner sei $a_1 + \cdots + a_n = m-1$. Fragt man dann nach der Anzahl der Elemente, welche $A_1, \cdots, A_n$ gemeinsam sind, ohne in C enthalten zu sein, so wird diese Anzahl wie folgt erhalten. Jeder irreduziblen Verwandtschaft V der Stufe s kann man zwei Polynome einer Variablen x zuordnen, etwa das erste Salmonsche Polynom, bez. das zweite Salmonsche Polynom von V genannt. Das erste ist $= x^{m-1} +$ einem Polynom vom Grade $m-1-s$, das zweite vom Grade s. Die Koeffizienten dieser Polynome sind aber nicht Zahlen, sondern Operatoren des Differenzenkalküls nach Art der oben definierten Hilbertschen Operatoren. Beispielsweise ist das zweite Salmonsche Polynom einer Form der Ordnungen $n_1, \cdots, n_k$ einfach $x + \Delta_{n_1, \ldots, n_k}$. Die obige Anzahl ist dann erhältlich, indem man das erste Salmonsche Polynom von C multipliziert mit den zweiten Salmonschen Polynomen der $A_1, \cdots, A_n$ und mit dem Koeffizient x^{m-1} auf $\varphi(r_1, \cdots, r_k)$ operiert.

53. Eine dritte wichtige Anwendung der aufgestellten Sätze ruht in ihrer Fähigkeit, den bekannten Plückerschen Formeln der Ebene analoge Formeln leicht auffinden, richtig aussprechen und streng begründen zu lassen. So sind z. B. die Plückerschen Formeln selbst mit Hilfe des Symbols des Kap. III viel strenger und dabei einfacher aufzustellen, als

dies sonst geschieht, oder überhaupt ohne Hilfe jener Symbole geschehen könnte. Nach den Ausführungen des Kap. III über die Multiplizität von Lösungen ist die Formel für die Klasse einer reduziblen oder irreduziblen ebenen Kurve $f = 0$ genau

$$k = n(n-1) - \sum H\left(f, a_1 \frac{\partial f}{\partial x_1} + a_2 \frac{\partial f}{\partial x_2} + a_3 \frac{\partial f}{\partial x_3}\right)_{A_i},$$

wobei die Summation rechts über alle singulären Punkte A_i von f auszudehnen ist, n die Ordnung von f, a_1, a_2, a_3 unbestimmte Parameter bedeuten. Die sogenannte erste Plückersche Formel $k = n(n-1) - 2d - 3r$ ergibt sich aus obiger dann durch die Annahme, daß $f = 0$ als Singularitäten nur Doppelpunkte und Spitzen zulasse, wobei für einen Doppelpunkt

$$H\left(f, a_1 \frac{\partial f}{\partial x_1} + \cdots\right)_A = 2,$$

für eine allgemeine Spitze

$$H\left(f, a_1 \frac{\partial f}{\partial x_1} + \cdots\right)_A = 3$$

sich leicht herleitet. Ähnlich lautet die zweite Plückersche Formel für die Zahl der Wendetangenten w richtig

$$w = 3n(n-2) - \sum H(f, D)_{A_i},$$

wo D die Hessesche Form von f bedeutet und die Summation wieder über alle singulären Punkte A_i von f auszudehnen ist. Die spezielle Form derselben $w = 3n(n-2) - 6d - 8r$ ergibt sich leicht ebenso wie die spezielle Form der ersten Plückerschen Formel, z. B. durch Diskussion eines Systems Noetherscher Bedingungen.

Genau so wie die obigen Formeln lassen sich Analoga entwickeln für die verschiedensten Berührungsprobleme in der Algebra eines Raumes oder einer Gruppe von Räumen. Beispielsweise ist die Zahl der durch eine gegebene Gerade gehenden Ebenen, die eine gegebene Oberfläche $f = 0$ berühren

$$n(n-1)^2 - \sum H\left(f, a_1 \frac{\partial f}{\partial x_1} + \cdots, b_1 \frac{\partial f}{\partial x_1} + \cdots\right)_{A_i},$$

wo n die Ordnung der Oberfläche, A_i die singulären Punkte derselben, a_i, b_i unbestimmte Konstante sind. Dabei ist aber vorausgesetzt, daß die Singularitäten nur in endlicher Zahl vorkommen. Eine Spezialisation zeigt, daß einem r-fachen Punkte A im allgemeinen die Zahl

$$H\left(f, a_1 \frac{\partial f}{\partial x_1} + \cdots, b_1 \frac{\partial f}{\partial x_1} + \cdots\right)_A = r(r-1)^2$$

entspricht. Ist $r = 2$ und zerfällt der Tangentenkegel bei A, so ist im allgemeinen $H(f, \cdots)_A = 3$; ist der Tangentenkegel das Quadrat einer

Ebene, so ist $H(f, \cdots)_A = 4$ etc. etc. Enthält $f = 0$ Kurven von Singularitäten, so treten die Begriffe und Sätze des Salmonschen Problems in Kraft. Allemal bieten die Methoden der vorliegenden Arbeit die Mittel zur allgemeinen Lösung der betreffenden Probleme — seien dieselben auf Formen, oder auf Gebilde höherer Stufe, oder auf die Singularitäten (z. B. sogenannte Fundamentalpunkte etc.) von Verwandtschaften beliebiger Stufen bezüglich. —

Als das aus der vorliegenden Arbeit emporwachsende Hauptproblem möchte ich die Bestimmung der geometrischen Bedeutung aller Koeffizienten der Hilbertschen Funktion eines Moduls, insbesondere eines Primmoduls, bezeichnen. Man weiß z. B., daß, wenn für große R die Hilbertsche Funktion einer irreduziblen Raumkurve $aR - b$ ist, und die Raumkurve keine Doppelpunkte hat, dann $b + 1$ das Geschlecht der Kurve angibt. Die analoge Frage könnte man aufwerfen für die Koeffizienten der Noether-Hilbertschen Funktion eines analytischen Moduls, wie für die Indizes der „Elementarteiler" eines Ideals.

Charlottenburg, März 1904.

Inhaltsverzeichnis.