

# Zur Theorie der Polynomideale und Resultanten.

Von

Kurt Hentzelt †.

Bearbeitet von Emmy Noether in Göttingen<sup>1)</sup>.

Es handelt sich im folgenden um das *allgemeine Problem der Eliminationstheorie, die gemeinsamen Nullstellen aller Polynome eines Ideals aus Polynomen zu bestimmen*; oder was damit identisch ist, die Nullstellen irgendeiner endlichen Anzahl von Polynomen, die eine Basis des Ideals bilden; dabei wird sich zugleich eine begriffliche Deutung der auftretenden Multiplizitäten ergeben. Die Koeffizienten der Polynome können irgendeinem Körper zugewiesen werden, die Nullstellen gehören dann dem daraus abgeleiteten algebraisch abgeschlossenen Körper an. Außerdem kann das Ideal ohne Beschränkung der Allgemeinheit als transformiertes (§ 3) angenommen werden. Dann ist das wesentliche Resultat das folgende:

*Jedem Ideal  $m$  aus Polynomen läßt sich eine Resultantenform zuordnen:*

$$R_m = R^{(1)}(x_1 \dots x_n) \cdot \dots \cdot R^{(i)}(x_1 \dots x_n) \cdot \dots \cdot R^{(n)}(x_n) \equiv 0 (m)$$

---

<sup>1)</sup> Kurt Hentzelt ist seit Oktober 1914 von Dirmuiden vermißt und muß zu den Toten gezählt werden. Die hier gegebene Abhandlung ist eine vollständig freie Bearbeitung des wesentlichsten Teiles seiner Dissertation „Zur Theorie der Formenmoduln und Resultanten“, mit der er im Sommer 1914 bei E. Fischer in Erlangen promovierte. Diese ganz auf Grund eigener Ideen verfaßte Dissertation ist lückenlos aufgebaut; aber Hilfssatz reiht sich an Hilfssatz, alle Begriffe sind durch Formeln mit vier und fünf Indizes umschrieben, der Text fehlt fast vollständig, so daß dem Verständnis die größten Schwierigkeiten bereitet werden. Zu der geplanten Umarbeitung ist er selbst nicht mehr gekommen.

Ich gebe die Arbeit in rein begrifflicher Fassung wieder, wodurch eine große Vereinfachung der durchweg in den Grundgedanken auf Hentzelt zurückgehenden Beweise erzielt wird, und, wie ich hoffe, die Schönheit der Arbeit offenbar wird. Die Teile der Dissertation, die sich — bei gegebener Basis — auf die Frage der Bildung der auftretenden Funktionen durch endlich viele Schritte beziehen, sollen einer gesonderten Veröffentlichung vorbehalten bleiben. (E.N.)

derart, daß  $R_m$  für alle Nullstellen von  $m$  und nur für diese verschwindet. Ist  $n$  ein Teiler von  $m$ , und stimmen die Resultantenformen  $R_n$  und  $R_m$  überein, so stimmen auch die Ideale  $n$  und  $m$  überein.

Der zweite Teil des Hauptsatzes zeigt, daß die Resultantenform die Nullstellen in charakteristischer Multiplizität liefert. Dieser zweite Teil ist ein Analogon dazu, daß zwei Ideale eines algebraischen Zahlkörpers, von denen eines ein Teiler des andern ist, dann und nur dann übereinstimmen, wenn ihre Normen übereinstimmen; auch der innere Grund beider Sätze ist der gleiche.

Es läßt sich nämlich  $m$  als Linearformenmodul  $\mathfrak{M}_{i-1}$  auffassen, indem man jedes Polynom als Linearform in den Potenzprodukten von  $x_1 \dots x_{i-1}$  auffaßt und  $x_{i+1} \dots x_n$  dem Koeffizientenbereich adjungiert. Der Resultantenfaktor  $R^{(6)}$  wird dann gleich der Norm des zugehörigen Grundmoduls (§ 1)  $\mathfrak{G}_{i-1}$  nach  $\mathfrak{M}_{i-1}$ , wodurch sich auch sofort eine Deutung der Multiplizität — Produkt von Grad und Exponent eines Faktors von  $R^{(6)}$  — durch die Anzahl linear unabhängiger Restklassen ergibt<sup>2)</sup>, eine Tatsache, die bis jetzt nur in dem speziellen Fall bekannt war, wo die Resultante sich für unbestimmte Koeffizienten definieren läßt<sup>3)</sup>.

Zur Ableitung dieser Resultate werden in § 1 und 2 Sätze über Moduln aus Linearformen gegeben, deren Koeffizienten ganze rationale Zahlen oder Polynome einer Unbestimmten sind. Den Zusammenhang mit den in § 3 eingeführten Idealen aus Polynomen vermittelt der Isomorphiesatz des § 4. § 5 gibt den oben erwähnten zweiten Teil des Hauptsatzes, § 7 den Satz über die Nullstellen, dem in § 6 eine allgemeine Eliminationstheorie vorausgeht. Hier wird zugleich, bei Einführung neuer Unbestimmten, die Zerlegung der Resultante in Linearformen dieser Unbestimmten bewiesen; und damit bei der hier gegebenen Elimination ein einwandfreier Beweis für eine Kroneckersche Behauptung erbracht<sup>4)</sup>.

<sup>2)</sup> Diese letzteren Resultate zeigen ihre eigentliche Bedeutung, wenn man die Zerlegung der Ideale in primäre heranzieht; die einem primären Ideal entsprechende Multiplizität ist dann definiert als Anzahl der linear unabhängigen Restklassen des Komplements nach diesem Ideal; darauf soll an anderer Stelle eingegangen werden. (E. N.)

<sup>3)</sup> Vgl. Macaulay, The algebraic theory of modular systems, Cambridge Tracts 19 (Cambridge University Press, 1916); Nr. 67; auch Lasker, Zur Theorie der Moduln und Ideale, Math. Ann. 60 (1905), S. 20–116; S. 98. Daß in diesem Fall Resultante und Resultantenform übereinstimmt, ist in den unter <sup>1)</sup> erwähnten, noch nicht veröffentlichten Sätzen von Hentzelt gezeigt. (E. N.)

<sup>4)</sup> Der versuchte Beweis bei König, Algebraische Größen (Leipzig 1908, Teubner), V, § 4 — für die Kroneckersche Eliminationstheorie — ist bekanntlich nicht gelungen. Daß auch bei den von König in die Kroneckersche Eliminationstheorie eingeführten Multiplizitäten der zweite Teil des Hentzeltschen Hauptsatzes nicht gilt, zeigt Macaulay a. a. O. S. 28, wo weiter gezeigt wird, daß die Kroneckersche Eliminationstheorie nicht der Zerlegung in primäre Ideale entspricht. (E. N.)

## § 1.

## Moduln aus Linearformen.

Unter ganzen Größen  $a, b, c, \dots$  werden in den beiden ersten Paragraphen ganze rationale Zahlen oder Polynome einer Unbestimmten mit Koeffizienten aus einem beliebigen, abstrakt definierten Körper  $P$  verstanden; unter Linearformen  $a(\xi), b(\xi), \dots$  solche in endlich viel Unbestimmten  $\xi_1 \dots \xi_k$  mit ganzen Größen als Koeffizienten.

Ein Modul  $\mathfrak{A}$  aus Linearformen ist definiert durch die Bedingungen:  $\mathfrak{A}$  enthält neben  $a(\xi)$  und  $b(\xi)$  auch die Differenz  $a(\xi) - b(\xi)$ ; neben  $a(\xi)$  auch  $c \cdot a(\xi)$ , unter  $c$  eine beliebige ganze Größe verstanden.

Unter dem Rang von  $\mathfrak{A}$  verstehen wir, wie üblich, die Maximalzahl von linear unabhängigen Linearformen aus  $\mathfrak{A}$ ; unter dem  $\lambda$ -ten Determinantenteiler  $d_\lambda$  von  $\mathfrak{A}$  den größten gemeinsamen Teiler aller Determinanten  $\lambda$ -ten Grades aus  $\mathfrak{A}$  (d. h. aller Determinanten  $\lambda$ -ten Grades, die sich aus der Koeffizientenmatrix von je  $\lambda$  Linearformen aus  $\mathfrak{A}$  bilden lassen). Ist  $\varrho$  der Rang von  $\mathfrak{A}$ , also  $d_1, \dots, d_\varrho$  die von Null verschiedenen Determinantenteiler, so sind die Elementarteiler von  $\mathfrak{A}$  definiert durch  $e_1 = d_1$ ;  $e_2 = d_2/d_1$ ;  $\dots$ ;  $e_\varrho = d_\varrho/d_{\varrho-1}$ ;  $e_{\varrho+i} = 0$ .  $\mathfrak{A}$  ist bekanntlich ein endlicher Modul, der eine Modulbasis aus genau  $\varrho$  Linearformen  $a_1(\xi), \dots, a_\varrho(\xi)$  besitzt, durch die sich jede Linearform aus  $\mathfrak{A}$  linear, mit ganzen Größen als Koeffizienten, darstellen läßt:  $\mathfrak{A} = (a_1(\xi), \dots, a_\varrho(\xi))$ . Bedeutet  $A$  die Koeffizientenmatrix dieser Linearformen, so stimmen daher die Determinanten- und Elementarteiler von  $\mathfrak{A}$  mit denen von  $A$  überein, woraus zunächst folgt, daß jeder Elementarteiler  $e_\lambda$  im folgenden  $e_{\lambda+1}$  aufgeht. Die nach der Elementarteilertheorie bestehende Matrizengleichung

$$PAQ = \begin{pmatrix} e_1 & & \\ & \ddots & \\ & & e_\varrho \end{pmatrix}$$

zeigt weiter — wenn durch unimodulare Transformation  $\xi = Q(\eta)$  neue Unbestimmten  $\eta_1 \dots \eta_k$  eingeführt werden — das Bestehen der Modulgleichung:

$$(1) \quad \mathfrak{A} = (e_1 \eta_1, e_2 \eta_2, \dots, e_\varrho \eta_\varrho).$$

Der für das folgende wesentlichste Begriff ist der des Grundmoduls<sup>5)</sup>, nach

<sup>5)</sup> Vgl. Steinitz, Rechteckige Systeme und Moduln in algebraischen Zahlkörpern *Math. Ann.* 72 (1912), S. 297–345, Nr. 36. Hentzelt scheint aber jedenfalls unabhängig von Steinitz, mit dem sich auch sonst Berührungspunkte finden, für seinen einfachen Fall zu dem Begriff, in der Fassung von Formel (4), gekommen zu sein. (Vgl. Anm.)

Definition I. Ein Modul  $\mathfrak{G}$  heißt Grundmodul, wenn er keinen echten Teiler gleichen Ranges besitzt<sup>a)</sup>.

$\mathfrak{G}$  ist also dann und nur dann Grundmodul, wenn aus

$$(2) \quad c \cdot g(\xi) \equiv 0(\mathfrak{G}); \quad c \neq 0 \text{ stets folgt: } g(\xi) \equiv 0(\mathfrak{G}).$$

Der Zusammenhang zwischen beliebigem Modul und Grundmodul wird gegeben durch

Satz I. Jeder Modul  $\mathfrak{A}$  ist durch einen und nur einen Grundmodul  $\mathfrak{G}$  gleichen Ranges teilbar;  $\mathfrak{G}$  ist definiert als kleinster Teiler gleichen Ranges von  $\mathfrak{A}$  und dargestellt durch

$$(3) \quad \mathfrak{G} = (\eta_1, \dots, \eta_e);$$

$\mathfrak{G}$  soll als Grundmodul von  $\mathfrak{A}$  bezeichnet werden.

Die Bedingung, daß  $\mathfrak{G}$  der kleinste Teiler gleichen Ranges sein soll, drückt sich nämlich so aus:  $\mathfrak{G}$  enthält alle und nur die Linearformen  $g(\xi)$ , die einer Relation genügen

$$(4) \quad b \cdot g(\xi) \equiv 0(\mathfrak{A}); \quad b \neq 0.$$

Daraus ergibt sich zunächst, daß  $\mathfrak{G}$  Modul ist, da neben

$$b_1 g_1(\xi) \equiv 0(\mathfrak{A}); \quad b_1 \neq 0; \quad b_2 g_2(\xi) \equiv 0(\mathfrak{A}); \quad b_2 \neq 0$$

auch

$$b_1 b_2 (g_1(\xi) - g_2(\xi)) \equiv 0(\mathfrak{A}); \quad b_1 b_2 \neq 0$$

erfüllt ist; und natürlich auch  $b_1 \cdot c g_1(\xi) \equiv 0(\mathfrak{A})$ .  $\mathfrak{G}$  ist aber auch Grundmodul; denn aus

$$c \cdot g(\xi) \equiv 0(\mathfrak{G}); \quad c \neq 0$$

folgt nach (4):

$$b c g(\xi) \equiv 0(\mathfrak{A}); \quad b c \neq 0,$$

also wieder nach (4) auch  $g(\xi) \equiv 0(\mathfrak{G})$ .

Es gibt ferner keinen von dem kleinsten Teiler gleichen Ranges  $\mathfrak{G}$  verschiedenen Grundmodul  $\mathfrak{G}_1$ , der den Bedingungen genügt. Denn  $\mathfrak{G}_1$  müßte durch  $\mathfrak{G}$  teilbar sein, besitzt aber als Grundmodul keinen echten Teiler gleichen Ranges, und ist somit mit  $\mathfrak{G}$  identisch. Schließlich ist der durch die rechte Seite von (3) dargestellte Modul Grundmodul, da jeder echte Teiler eine weitere Unbestimmte  $\eta$  enthalten muß, also höheren Rang besitzt; und somit ergibt (3) den eindeutig definierten Grundmodul von  $\mathfrak{A}$ , womit Satz I in allen Teilen bewiesen ist.

<sup>a)</sup> Teiler im Modulsinn verstanden:  $\mathfrak{A}$  ist teilbar durch  $\mathfrak{B}$ ,  $\mathfrak{A} \equiv 0(\mathfrak{B})$ , wenn jedes Element aus  $\mathfrak{A}$  in  $\mathfrak{B}$  enthalten ist;  $\mathfrak{B}$  heißt echter Teiler, wenn es von  $\mathfrak{A}$  verschiedene Elemente enthält.

Ein weiterer für das folgende wesentlicher Begriff ist der Dedekindsche Begriff des Quotienten zweier Moduln<sup>7)</sup> nach

Definition II. Der Quotient  $c = \mathfrak{A}/\mathfrak{B}$  zweier Moduln aus Linearformen ist definiert als Gesamtheit der ganzen Größen  $c$ , die der Bedingung

$$c \cdot \mathfrak{B} \equiv 0(\mathfrak{A})$$

genügen.  $c$  stellt ein Ideal aus ganzen Größen, also ein Hauptideal dar. Entsprechend ist der Quotient  $\mathfrak{C} = \mathfrak{A}/b$  eines Moduls  $\mathfrak{A}$  aus Linearformen durch ein Ideal  $b$  aus ganzen Größen definiert als Gesamtheit der Linearformen  $c(\xi)$ , die der Bedingung

$$c(\xi) \cdot b \equiv 0(\mathfrak{A})$$

genügen.  $\mathfrak{C}$  stellt wieder einen Modul aus Linearformen dar, und zwar, sobald  $b$  vom Nullideal verschieden ist, einen Modul gleichen Ranges wie  $\mathfrak{A}$ .

Dazu ist nur zu bemerken, daß es nach der Definition klar ist, daß dem Quotienten jeweils die Moduleigenschaft zukommt; Systeme aus ganzen Größen mit Moduleigenschaft sind aber Ideale.

Der Quotientenbegriff führt zu einem Zusammenhang zwischen Grundmodul und höchstem Elementarteiler, nach

Satz II. Zwischen Grundmodul und höchstem Elementarteiler von  $\mathfrak{A}$  besteht die reziproke Beziehung

$$(5) \quad (e_e) = \mathfrak{A}/\mathfrak{G}; \quad \mathfrak{G} = \mathfrak{A}/(e_e),$$

wo  $(e_e)$  das aus  $e_e$  abgeleitete Hauptideal bedeutet.

Denn da jeder Elementarteiler in  $e_e$  aufgeht, so kommt nach (1) und (3):

$$(6) \quad e_e \mathfrak{G} \equiv 0(\mathfrak{A}) \quad \text{und folglich} \quad (e_e) \cdot \mathfrak{G} \equiv 0(\mathfrak{A});$$

es wird also  $(e_e)$  durch den Quotienten  $\mathfrak{A}/\mathfrak{G}$  teilbar. Es gilt aber auch das Umgekehrte; denn aus

$$b \mathfrak{G} \equiv 0(\mathfrak{A}) \quad \text{folgt} \quad b \eta_e \equiv 0(\mathfrak{A}) \quad \text{und somit} \quad b \equiv 0(e_e),$$

womit die erste Formel (5) bewiesen ist<sup>8)</sup>. (6) zeigt weiter, daß  $\mathfrak{G}$  durch

<sup>7)</sup> Bei Dedekind handelt es sich um Zahlenmoduln, für die auch eine Multiplikation definiert ist, so daß der Dedekindsche Quotient nicht mit dem hier definierten Quotienten übereinstimmt. (E. N.)

<sup>8)</sup> Setzt man  $\mathfrak{A}_0 = \mathfrak{A}$ , ...,  $\mathfrak{A}_i = (\mathfrak{A}, \eta_e, \dots, \eta_{e-i+1})$ , wo also jeweils  $\mathfrak{A}_i$  den höchsten Elementarteiler  $e_{e-i}$  besitzt, so kommt nach denselben Schlüssen:

$$(e_e) = \mathfrak{A}_0/\mathfrak{A}_1, \dots, (e_{e-1}) = \mathfrak{A}_1/\mathfrak{A}_{i+1}, \dots, (e_i) = \mathfrak{A}_{e-i-1}/\mathfrak{A}_e.$$

Selbstverständlicher:  $\zeta_i = b_{i1} \eta_1 + \dots + b_{i,i} \eta_i$  gesetzt, sei  $(b_{i1}, e_i) = \mathfrak{F}$  und bedeute

$$\mathfrak{B}_0 = \mathfrak{A}, \dots, \mathfrak{B}_i = (\mathfrak{A}, \zeta_e, \dots, \zeta_{e-i+1}),$$

so besitzt auch  $\mathfrak{B}_i$  den höchsten Elementarteiler  $e_{e-i}$ , und es kommt somit

$$(e_{e-i}) = \mathfrak{B}_i/\mathfrak{B}_{i+1}.$$

den Quotienten  $\mathfrak{A}/(e_\varrho)$  teilbar ist; dieser Quotient ist ein Teiler gleichen Ranges von  $\mathfrak{A}$ , also nach der Definition des Grundmoduls von  $\mathfrak{A}$  auch umgekehrt durch  $\mathfrak{G}$  teilbar, womit auch die zweite Formel (5) bewiesen ist.

Bedeutet  $d$  irgendeine nicht identisch verschwindende Determinante  $\varrho$ -ten Grades aus  $\mathfrak{A}$ , so wird  $d$  durch den  $\varrho$ -ten Determinantenteiler  $d_\varrho$  und folglich durch  $e_\varrho$  teilbar; es kommt also  $d\mathfrak{G} \equiv 0(\mathfrak{A})$  und nach dem obigen Schluß folgt daraus  $\mathfrak{G} = \mathfrak{A}/(d)$ . Es ist aber für das Spätere wesentlich, daß diese letztere Quotientendarstellung für  $\mathfrak{G}$  sich auch ohne Zurückgehen auf die Elementarteiler beweisen läßt, und daher allgemeinere Gültigkeit besitzt, nach

**Satz III.** *Versteht man unter ganzen Größen Polynome in mehreren Unbestimmten<sup>9)</sup>, so gilt noch die Quotientendarstellung*

$$(7) \quad \mathfrak{G} = \mathfrak{A}/(d),$$

*unter  $d$  irgendeine nicht identisch verschwindende Determinante  $\varrho$ -ten Grades aus  $\mathfrak{A}$  verstanden.*

Vorerst ist klar, daß die Begriffe des Ranges, des Grundmoduls und des Modulquotienten — der nur jetzt kein Hauptideal wird — bei dieser Erweiterung erhalten bleiben, ferner Satz I mit Ausnahme der Basisdarstellung.

Es seien jetzt

$$a_1(\xi) = a_{11}\xi_1 + \dots + a_{1k}\xi_k; \dots; a_\varrho(\xi) = a_{\varrho 1}\xi_1 + \dots + a_{\varrho k}\xi_k$$

$\varrho$  linear unabhängige Linearformen aus  $\mathfrak{A}$ , die im allgemeinen keine Modulbasis bilden werden; die Unbestimmten  $\xi$  seien so bezeichnet, daß

$$d = |a_{ij}| \neq 0; \quad i, j = 1, 2, \dots, \varrho.$$

Hieraus folgt, daß  $\varrho$  Linearformen von spezieller Gestalt zu  $\mathfrak{A}$  gehören:

$$(8) \quad d\xi_1 + b_{\lambda, \varrho+1}\xi_{\varrho+1} + \dots + b_{\lambda, k}\xi_k \equiv 0(\mathfrak{A}) \quad (\lambda = 1, 2, \dots, \varrho).$$

$\mathfrak{A}$  kann aber keine nur von  $\xi_{\varrho+1} \dots \xi_k$  abhängige Linearform  $c_{\varrho+1}\xi_{\varrho+1} + \dots + c_k\xi_k$  enthalten, da sonst mindestens eine  $(\varrho+1)$ -reihige Determinante  $d \cdot c_\sigma$  von Null verschieden wäre.

<sup>9)</sup> Tatsächlich wird nur benutzt, daß die ganzen Größen sich durch Addition, Subtraktion und Multiplikation reproduzieren, unter Gültigkeit der gewöhnlichen Rechnungsregeln, daß sie also einen Ring bilden; und weiter, daß in diesem Ring ein Produkt nur verschwindet, wenn ein Faktor verschwindet, daß der Ring sich also durch Quotientenbildung (Adjunktion von Elementenpaaren) zu einem Körper erweitern läßt. Dagegen wird keine Basisdarstellung des Moduls benutzt, (7) gilt also z. B. auch für den Bereich aller ganzen algebraischen Zahlen als Koeffizienten. (E. N.)

Nun ist der Quotient  $\mathfrak{A}/(d)$  als Teiler gleichen Ranges von  $\mathfrak{A}$  durch  $\mathfrak{G}$  teilbar; es gilt aber auch das Umgekehrte. Denn für jedes  $g(\xi) \equiv 0(\mathfrak{G})$  gilt nach Definition:

$$c \cdot g(\xi) \equiv 0(\mathfrak{A}); \quad c \neq 0 \quad \text{und folglich} \quad d \cdot c \cdot g(\xi) \equiv 0(\mathfrak{A}).$$

Nach (8) wird aber

$$d \cdot g(\xi) = g_{\varrho+1} \xi_{\varrho+1} + \dots + g_k \xi_k(\mathfrak{A}),$$

folglich kommt

$$c g_{\varrho+1} \xi_{\varrho+1} + \dots + c g_k \xi_k \equiv 0(\mathfrak{A}),$$

also nach dem eben Bemerkten  $c \cdot g_{\varrho+1} = 0, \dots, c \cdot g_k = 0$  und damit, wegen  $c \neq 0$ , auch  $g_{\varrho+1} = 0, \dots, g_k = 0$ , also  $d \cdot g(\xi) \equiv 0(\mathfrak{A})$ , womit (7) bewiesen ist.

Es sei bemerkt, daß  $d \cdot g(\xi) \equiv 0(\mathfrak{A})$  auch direkt daraus folgt, daß die beiden Moduln  $(a_1(\xi), \dots, a_{\varrho}(\xi))$  und  $(g(\xi), a_1(\xi), \dots, a_{\varrho}(\xi))$  gleichen Rang  $\varrho$  besitzen, so daß also —  $g(\xi) = c_1 \xi_1 + \dots + c_k \xi_k$  gesetzt — die  $(\varrho + 1)$ -reihige Determinante

$$\begin{vmatrix} a_1(\xi) & a_{11} & \dots & a_{1\varrho} \\ \vdots & \vdots & & \vdots \\ a_{\varrho}(\xi) & a_{\varrho 1} & \dots & a_{\varrho \varrho} \\ g(\xi) & c_1 & \dots & c_{\varrho} \end{vmatrix}$$

verschwindet. Der oben gegebene Beweis kehrt aber in § 4, im Anschluß an Formel (30), wieder.

## § 2.

### Zerlegungssätze für Normen und Moduln.

Es handelt sich jetzt wieder um Linearformen-Moduln in bezug auf ganze rationale Zahlen oder Polynome einer Unbestimmten mit Koeffizienten aus  $P$ .

**Definition III.** *Faßt man, wie üblich, alle diejenigen Linearformen in  $\xi$ , die modulo  $\mathfrak{A}$  einander kongruent sind, in eine Restklasse zusammen, so bezeichne das Symbol  $\mathfrak{G}|\mathfrak{A}$  das System der Restklassen von  $\mathfrak{G}$  nach  $\mathfrak{A}$ , d. h. das System all derjenigen Restklassen nach  $\mathfrak{A}$ , die aus Elementen von  $\mathfrak{G}$  bestehen. Die Norm von  $\mathfrak{G}$  nach  $\mathfrak{A}$  — in Zeichen  $N(\mathfrak{G}|\mathfrak{A})$  — ist definiert als Determinante der Übergangssubstitution von  $\mathfrak{G}$  nach  $\mathfrak{A}$ , d. h. als Determinante der Substitution, die irgendeine linear unabhängige Modulbasis von  $\mathfrak{A}$  durch eine ebensolche des Grundmoduls  $\mathfrak{G}$  von  $\mathfrak{A}$  ausdrückt.*

Aus (1) und (3) bzw. der Bemerkung zu Satz II ergibt sich:

$$(9) \quad N(\mathfrak{G}|\mathfrak{A}) = e_1 e_2 \dots e_{\varrho} = d_{\varrho}; \quad \mathfrak{G} = \mathfrak{A}/(N(\mathfrak{G}|\mathfrak{A})).$$

Aus (1), (3) und (9) folgt in bekannter Weise, daß  $N(\mathfrak{G}|\mathfrak{A})$  im Fall ganzer rationaler Zahlen die Anzahl der Restklassen von  $\mathfrak{G}$  nach  $\mathfrak{A}$  darstellt, während im Fall von Polynomen einer Unbestimmten — wo die Anzahl der Restklassen im allgemeinen unendlich wird — der Grad von  $N(\mathfrak{G}|\mathfrak{A})$  gleich der Anzahl der in bezug auf  $P$  linear unabhängigen Restklassen wird. Ist  $\mathfrak{B}$  ein Teiler gleichen Ranges von  $\mathfrak{A}$ , so enthält  $\mathfrak{B}$  neben einem Repräsentanten irgendeiner solchen Restklasse zugleich alle Elemente der Restklasse, entsteht also durch Zufügung von endlich vielen Restklassen bzw. ihrer linearen Verbindungen zu  $\mathfrak{A}$ . Daraus folgt sofort:

**Satz IV.** *Ist  $\mathfrak{B}$  ein Teiler gleichen Ranges von  $\mathfrak{A}$ , so daß also die Grundmoduln übereinstimmen, und wird außerdem  $N(\mathfrak{G}|\mathfrak{B}) = N(\mathfrak{G}|\mathfrak{A})$ , so wird auch  $\mathfrak{B} = \mathfrak{A}$ .*

Über den Zusammenhang der Zerlegung von Normen und Moduln gilt

**Satz V.** *Es sei*

$$(10) \quad N(\mathfrak{G}|\mathfrak{A}) = r \cdot s, \quad (r, s) = 1;$$

*dann existiert ein und nur ein Modul  $\mathfrak{R}$ , ebenso ein und nur ein Modul  $\mathfrak{S}$ , die beide Teiler gleichen Ranges von  $\mathfrak{A}$  sind, derart, daß*

$$r = N(\mathfrak{G}|\mathfrak{R}), \quad s = N(\mathfrak{G}|\mathfrak{S})$$

*wird.  $\mathfrak{R}$  und  $\mathfrak{S}$  sind definiert als*

$$\mathfrak{R} = \mathfrak{A}/(s); \quad \mathfrak{S} = \mathfrak{A}/(r),$$

*und es wird  $\mathfrak{A}$  gleich dem kleinsten gemeinsamen Vielfachen von  $\mathfrak{R}$  und  $\mathfrak{S}$ .<sup>10)</sup>*

*Setzt man  $r_e = (r, e_e)$ ;  $s_e = (s, e_e)$ , so gelten die Reziprozitäten*

$$(11) \quad (s_e) = \mathfrak{A}/(\mathfrak{R}); \quad \mathfrak{R} = \mathfrak{A}/(s_e); \quad (r_e) = \mathfrak{A}/(\mathfrak{S}); \quad \mathfrak{S} = \mathfrak{A}/(r_e).$$

Setzt man nämlich allgemein  $r_i = (r, e_i)$ ,  $s_i = (s, e_i)$ , so kommt nach (9) und (10):

$$(r_i, s_i) = 1; \quad e_i = r_i s_i; \quad r = r_1 \dots r_e; \quad s = s_1 \dots s_e,$$

und jedes  $r_i$  bzw.  $s_i$  geht im folgenden  $r_{i+1}$  bzw.  $s_{i+1}$  auf.

Setzt man also

$$\mathfrak{R} = (r_1 \eta_1, \dots, r_e \eta_e); \quad \mathfrak{S} = (s_1 \eta_1, \dots, s_e \eta_e),$$

so werden  $\mathfrak{R}$  und  $\mathfrak{S}$  Teiler gleichen Ranges von  $\mathfrak{A}$ ;  $\mathfrak{A}$  wird wegen der Teilerfremdheit von  $r_i$  und  $s_i$  gleich dem kleinsten gemeinsamen Vielfachen von  $\mathfrak{R}$  und  $\mathfrak{S}$ , und es kommt ferner

$$N(\mathfrak{G}|\mathfrak{R}) = r_1 \dots r_e = r; \quad N(\mathfrak{G}|\mathfrak{S}) = s_1 \dots s_e = s.$$

<sup>10)</sup> Kleinstes gemeinsames Vielfaches  $[\mathfrak{R}, \mathfrak{S}]$  im Modulsinn verstanden: Gesamtheit der Linearformen, die sowohl durch  $\mathfrak{R}$  wie durch  $\mathfrak{S}$  teilbar sind. Entsprechend ist der größte gemeinsame Teiler  $(\mathfrak{R}, \mathfrak{S})$  im Modulsinn zu verstehen als Gesamtheit der Linearformen, die sich darstellen lassen als Summe eines Elementes aus  $\mathfrak{R}$  und eines Elementes aus  $\mathfrak{S}$ .



Weiter gilt

$$s_e \mathfrak{R} \equiv 0(\mathfrak{A}); \quad r_e \mathfrak{S} \equiv 0(\mathfrak{A});$$

aus  $c \mathfrak{R} \equiv 0(\mathfrak{A})$  folgt  $c r_e \eta_e \equiv 0(\mathfrak{A})$ , also  $c \equiv 0(s_e)$ , womit  $(s_e) = \mathfrak{A}/\mathfrak{R}$  und entsprechend  $(r_e) = \mathfrak{A}/\mathfrak{S}$  bewiesen ist. Aus

$$b(\eta) = b_1 \eta_1 + \dots + b_e \eta_e \equiv 0(\mathfrak{A}/(s_e))$$

folgt wegen der Teilerfremdheit aller  $r_i$  zur  $s_e$  ferner  $b_i \equiv 0(r_i)$ , also  $\mathfrak{R} = \mathfrak{A}/(s_e)$  und entsprechend  $\mathfrak{S} = \mathfrak{A}/(r_e)$ , womit die Reziprozitäten (11) bewiesen sind, die für den Spezialfall  $r = 1$  in (5) übergehen.

Es ist noch die *eindeutige Bestimmtheit* von  $\mathfrak{R}$  und  $\mathfrak{S}$  zu zeigen. Seien  $\bar{\mathfrak{R}}$  und  $\bar{\mathfrak{S}}$  den Bedingungen von Satz V genügende Moduln,  $\bar{r}_i$  und  $\bar{s}_i$  ihre Elementarteiler. Da  $\bar{r}_i$  und  $\bar{s}_i$  Teiler von  $e_i$  sind, kommt wegen

$$r = \bar{r}_1 \dots \bar{r}_e, \quad s = \bar{s}_1 \dots \bar{s}_e, \quad (\bar{r}_i, \bar{s}_i) = 1$$

auch

$$e_i = \bar{r}_i \bar{s}_i, \quad \bar{r}_i = (r, e_i) = r_i, \quad \bar{s}_i = (s, e_i) = s_i,$$

$\bar{\mathfrak{R}}$  und  $\bar{\mathfrak{S}}$  stimmen also mit  $\mathfrak{R}$  und  $\mathfrak{S}$  in Elementarteiler und Grundmodul überein. Führt man daher vermöge einer unimodularen Substitution  $\eta = Q(\zeta)$  neue Unbestimmte  $\zeta$  ein, so wird

$$\bar{\mathfrak{R}} = (r_1 \zeta_1, \dots, r_e \zeta_e);$$

$$\mathfrak{A} = (r_1 s_1 (q_{11} \zeta_1 + \dots + q_{1e} \zeta_e), \dots, r_e s_e (q_{e1} \zeta_1 + \dots + q_{ee} \zeta_e)).$$

Aus  $\mathfrak{A} \equiv 0(\bar{\mathfrak{R}})$  kommt somit  $r_i s_i (q_{i1} \zeta_1 + \dots + q_{ie} \zeta_e) \equiv 0(\bar{\mathfrak{R}})$ ; also  $r_i s_i q_{ij} \equiv 0(r_j)$ . Wegen  $(r, s) = 1$  ergibt das  $r_i q_{ij} \equiv 0(r_j)$  oder  $\mathfrak{R} \equiv 0(\bar{\mathfrak{R}})$ . Da aber  $N(\mathfrak{G}|\mathfrak{R}) = N(\mathfrak{G}|\bar{\mathfrak{R}})$  ist, so kommt  $\mathfrak{R} = \bar{\mathfrak{R}}$  nach Satz IV, und entsprechend  $\mathfrak{S} = \bar{\mathfrak{S}}$ , womit Satz V in *allen Teilen bewiesen* ist.

### § 3.

#### Ideale aus Polynomen.

Es sei  $\bar{\mathfrak{m}}$  ein *Ideal aus Polynomen* der  $n$  Unbestimmten  $y_1 \dots y_n$ , mit Koeffizienten aus einem beliebigen, abstrakt definierten Körper  $P$ ; d. h.  $\bar{\mathfrak{m}}$  enthält neben  $\Phi_1(y)$  und  $\Phi_2(y)$  auch die Differenz  $\Phi_1(y) - \Phi_2(y)$ , neben  $\Phi(y)$  auch  $A(y) \cdot \Phi(y)$ , unter  $A(y)$  ein beliebiges Polynom mit Koeffizienten aus  $P$  verstanden<sup>11)</sup>.

Die  $y$  seien einer Transformation mit Unbestimmten als Koeffizienten unterworfen,

$$(12) \quad y = U(x); \quad \text{etwa} \quad \begin{cases} y_1 = x_1, \\ y_2 = u_{21} x_1 + x_2, \\ \vdots \\ y_n = u_{n1} x_1 + \dots + u_{n,n-1} x_{n-1} + x_n, \end{cases}$$

<sup>11)</sup> Die begrifflich sich ergebende Bezeichnung „Ideal“ anstatt des früher allgemein üblichen „Modul“ oder „Formenmodul“ erweist sich hier schon zur Unterscheidung von den Moduln aus Linearformen als notwendig. (E: N.)

und die Unbestimmten  $u_{\mu\nu}$  dem Koeffizientenbereich der Polynome adjungiert, der somit in einen Körper  $P(u)$  übergeht. Durch diese Adjunktion gehe  $\bar{m}$  über in  $\bar{m}_{(u)}$ ;  $\bar{m}_{(u)}$  enthält also neben den Polynomen  $\Phi_i(y)$  aus  $\bar{m}$  auch alle linearen Verbindungen  $\sum \alpha_i(u) \Phi_i(y)$  je endlich vieler  $\Phi_i$ , unter  $\alpha_i(u)$  rationale Funktionen der  $u_{\mu\nu}$  mit Koeffizienten aus  $P$  verstanden. Die  $\alpha_i(u)$  können, durch Multiplikation mit einem geeigneten Polynom in  $u$ , ohne Beschränkung der Allgemeinheit als Potenzprodukte in  $u$  angenommen werden. Es gilt also:

$$(13) \quad \sum \alpha_i(u) \Phi_i(y) \equiv 0(m_{(u)}); \quad \Phi_i(y) \equiv 0(\bar{m}) \quad \text{und umgekehrt.}$$

Vermöge (12) geht  $\bar{m}_{(u)}$  über in ein Ideal  $m$  aus Polynomen in  $x_1 \dots x_n$ ; mit Koeffizienten aus  $P(u)$ :

$$(14) \quad \bar{m}_{(u)} = m \quad \text{vermöge} \quad y = U(x).$$

Die Verbindung der Relationen (14) und (13) sagen das folgende aus:

$$(15) \quad \text{Aus } F(x) \equiv 0(m); \quad F(x) = \Phi(y) = \sum \alpha_i(u) \Phi_i(y) = \sum \alpha_i(u) F_i(x) \\ \text{folgt} \quad F_i(x) \equiv 0(\bar{m});$$

während aus (14) und (15) sich rückwärts wieder (13) ergibt.

**Definition IV.** Ideale  $m$  aus Polynomen in  $x_1 \dots x_n$  mit Koeffizienten aus  $P(u)$ , die den Relationen (15) genügen, also vermöge  $y = U(x)$  aus  $\bar{m}_{(u)}$  entstehen, seien als transformierte Ideale bezeichnet.

Die transformierten Ideale sind durch die Existenz regulärer Polynome ausgezeichnet; ein Polynom vom Grade  $r$  heißt regulär in bezug auf  $x_i$ , wenn es den Term  $x_i^r$  mit von Null verschiedenem Koeffizienten enthält; man sieht, daß die Polynome  $F_i(x)$  regulär in bezug auf  $x_i$  sind. Es wird sich im folgenden wesentlich darum handeln, diese transformierten Ideale als Moduln aus Linearformen in gewissen Potenzprodukten der  $x$  aufzufassen. Dazu ist der Begriff des Grundideals festzulegen, der später in den Grundmodul übergehen wird. Wir schicken eine von jetzt an durchweg festgehaltene Bezeichnung voraus:

**Bezeichnung.** Unter  $F^{(i)}, f^{(i)}, a^{(i)}, \dots$  seien durchweg Polynome der  $x$  verstanden, die von  $x_1 \dots x_{i-1}$  frei sind.

**Definition V.** Zu jedem Ideal  $m$  sind  $n$  Grundideale  $g_0, g_1, \dots, g_{n-1}$  definiert durch die Festsetzung: das Grundideal  $(i-1)$ -ter Stufe  $g_{i-1}$  enthält alle und nur die Polynome  $G(x)$ , für die es ein — im allgemeinen mit  $G(x)$  sich änderndes — Polynom  $b^{(i)}$  gibt, derart, daß

$$(16) \quad b^{(i)} G(x) \equiv 0(m); \quad b^{(i)} \neq 0.$$

Daß die  $g$  tatsächlich Ideale sind, entspricht genau dem Nachweis der Moduleigenschaft für  $\mathfrak{G}$  im Anschluß an Formel (4), wozu (16) das

Analogon bedeutet. Es wird  $g_i$  durch  $g_{i-1}$  teilbar, da jedes Polynom  $b^{(i+1)}$  zugleich ein  $b^{(i)}$  ist.

Für die Grundideale gilt:

**Satz VI.** *Die Grundideale von transformierten Idealen sind transformierte Ideale<sup>12)</sup>.*

Der Beweis beruht auf einem bekannten *Dedekind-Mertensschen Satze<sup>13)</sup>*: Seien  $a$  und  $b$  Unbestimmte, sei gesetzt

$$\sum a_{i_1 \dots i_s} z_1^{i_1} \dots z_s^{i_s} \cdot \sum b_{j_1 \dots j_t} z_1^{j_1} \dots z_t^{j_t} = \sum c(a, b)_{k_1 \dots k_r} z_1^{k_1} \dots z_r^{k_r},$$

$$\sum i \leq \nu, \quad \sum j \leq \mu, \quad \sum k \leq \nu + \mu;$$

bedeuten ferner  $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}$  die jeweils aus den  $a, b, c$  vermöge ganzer rationaler Zahlen abgeleiteten Moduln, so existiert ein Exponent  $q$  derart, daß die Identität gilt:

$$(17) \quad \mathfrak{A}^q \mathfrak{B} = \mathfrak{A}^{q-1} \mathfrak{C}.$$

Dabei besteht  $\mathfrak{A}^q$  aus den Potenzprodukten  $q$ -ter Dimension der  $a$  und deren ganzzahligen linearen Verbindungen.

Zum Beweise von Satz VI sei jetzt gesetzt:

$$(18) \quad \begin{cases} G(x) = \Gamma(y) = \sum \alpha_i(u) I_i(y) = \sum \alpha_i(u) G_i(x), \\ b^{(i)}(x) = \varphi(y) = \sum \beta_\mu(u) \varphi_\mu(y), \end{cases}$$

wo also  $\alpha_i(u)$  und  $\beta_\mu(u)$  Potenzprodukte der  $u$  bedeuten. Dann gilt nach (16), (14) und (18):

$$(19) \quad \sum \beta_\mu(u) \varphi_\mu(y) \cdot \sum \alpha_i(u) I_i(y) \equiv 0 (\bar{m}_{(u)}); \quad \sum \beta_\mu(u) \varphi_\mu(y) \neq 0.$$

Hier steht links das Produkt zweier Polynome in  $u$ , deren Koeffizienten die Polynome  $\varphi_\mu(y)$  und  $I_i(y)$  sind; die Koeffizienten des Produktpolynoms in  $u$  sind nach der rechten Seite von (19) Polynome aus  $\bar{m}$ . Ersetzt man also in (17) die  $a, b, c$  durch diese Polynome in  $y$ , so ergibt sich

$$\left\{ \sum \beta_\mu(u) \varphi_\mu(y) \right\}^q \cdot \Gamma_i(u) \equiv 0 (\bar{m}_{(u)}),$$

was nach (18) gleichbedeutend ist mit:

$$(20) \quad b^{(i)}(x)^q \cdot G_i(x) \equiv 0 (\mathfrak{m}); \quad G_i(x) \equiv 0 (g_{i-1}).$$

Die Relationen (16), (18) und (20) zeigen, daß die Grundideale  $g_{i-1}$  tatsächlich transformierte Ideale sind.

<sup>12)</sup> Satz VI wird erst in § 7 benützt.

<sup>13)</sup> Dedekind: Über einen arithmetischen Satz von Gauß, Mitt. d. deutsch. math. Ges. zu Prag 1892. F. Mertens: Über einen algebraischen Satz, Ber. d. Ak. d. Wissensch. Wien 101 (1892), S. 1560–1566. — Die Kroneckersche Erweiterung des Gaußschen Satzes auf Polynome mit unbestimmten Koeffizienten ist eine unmittelbare Folgerung dieses Satzes.

## § 4.

**Zusammenhang zwischen Idealen aus Polynomen und Moduln aus Linearformen.**

Um ein Ideal  $\mathfrak{M}$  aus Polynomen, das stets als transformiertes vorausgesetzt wird, als Modul  $\mathfrak{M}_{i-1}$  ( $i = 1 \dots n$ ) aus Linearformen aufzufassen, sind die einzelnen Polynome  $F(x)$  als Linearformen in den Potenzprodukten  $\xi_\lambda$  von  $x_1 \dots x_{i-1}$  zu betrachten:

$$F(x) = \sum a_\lambda^{(i)} \xi_\lambda,$$

unter  $a_\lambda^{(i)}$  nach der Bezeichnung von § 3 Polynome in  $x_i \dots x_n$  verstanden. Aus der Definition des Ideals folgt sofort, daß  $\mathfrak{M}_{i-1}$  Moduleigenschaft in bezug auf diese ganzen Größen  $a^{(i)}, b^{(i)}, \dots$  zukommt; da ferner die unendlich vielen Potenzprodukte  $\xi$  der  $x_1 \dots x_{i-1}$  nur *linear* auftreten, spielen sie wegen ihrer linearen Unabhängigkeit für  $\mathfrak{M}_{i-1}$  die Rolle von Unbestimmten. Jeder Modul  $\mathfrak{M}_{i-1}$  enthält unendlich viele Unbestimmte  $\xi$ , aber in jeder einzelnen Linearform treten nur endlich viele Unbestimmte auf. Ebenso soll jedes Grundideal  $\mathfrak{g}_{i-1}$  als Linearformenmodul  $\mathfrak{G}_{i-1}$  aufgefaßt werden, wo die Unbestimmten wieder die Potenzprodukte von  $x_1 \dots x_{i-1}$  sind. Für  $i = 1$  handelt es sich nur um *eine* Unbestimmte  $\xi_0$ , die der Einheit entspricht.

Man kann sich nun, worauf alles folgende beruht, trotz dieser unendlich vielen Unbestimmten  $\xi$  auf Linearformenmoduln in endlich vielen Unbestimmten beschränken nach

**Satz VII.** *Das Restklassensystem  $\mathfrak{G}_{i-1} | \mathfrak{M}_{i-1}$  ist isomorph einem Restklassensystem  $\mathfrak{G}_{i-1}^* | \mathfrak{M}_{i-1}^*$ , wo  $\mathfrak{M}_{i-1}^*$  einen Modul in endlich vielen Unbestimmten und  $\mathfrak{G}_{i-1}^*$  seinen Grundmodul bedeutet. Der Modul  $\mathfrak{M}_{i-1}$  besitzt — bei Adjunktion von  $x_{i+1} \dots x_n$  zu  $P(u)$  — nur endlich viele von 1 verschiedene Elementarteiler, die von 1 verschiedenen Elementarteiler von  $\mathfrak{M}_{i-1}^*$ .*

Dabei sind die Elementarteiler von  $\mathfrak{M}_{i-1}$  wie in Anmerkung \*) zu definieren.

Die in Satz VII auftretende Isomorphie beruht auf

**Definition V.** *Zwei Restklassensysteme heißen isomorph, wenn sie sich derart eineindeutig zuordnen lassen, daß der Differenz zweier Klassen die Differenz der entsprechenden Klassen zugeordnet ist; und dem Produkt einer Klasse mit einer ganzen Größe das Produkt der entsprechenden Klasse mit derselben ganzen Größe.*

Der Beweis von Satz VII ergibt sich durch *volle Induktion*. Für  $i = 1$  ist Satz VII offenbar richtig; denn  $\mathfrak{M}_0$  ist ein Linearformenmodul

in einer Unbestimmten  $\xi_0$ , die dem Potenzprodukt nullter Dimension der  $x$ , also der Einheit entspricht; ganze Größen sind alle Polynome von  $x_1 \dots x_n$ . Das Grundideal  $\mathfrak{g}_0$  wird gleich dem aus allen Polynomen von  $x_1 \dots x_n$  bestehenden Einheitsideal,  $\mathfrak{G}_0$  also gleich dem Modul  $(\xi_0)$ , dem Grundmodul von  $\mathfrak{M}_0$ , so daß hier  $\mathfrak{G}_0^* | \mathfrak{M}_0^*$  mit  $\mathfrak{G}_0 | \mathfrak{M}_0$  zusammenfällt. Schließlich kann  $\mathfrak{M}_0$ , als vom Rang 1, höchstens einen von 1 verschiedenen Elementarteiler besitzen.

Wir gehen vorerst von  $i=1$  zu  $i=2$  über, um mit der hier gewonnenen Einsicht in den Bau von  $\mathfrak{G}_1 | \mathfrak{M}_1$  den Induktionsschluß allgemein zu führen. Dazu zeigen wir zunächst, daß für  $\mathfrak{G}_0 | \mathfrak{M}_0$  ein in  $x_1$  beschränktes Repräsentantensystem genommen werden darf, was dann wegen der Teilbarkeit von  $\mathfrak{g}_1$  durch  $\mathfrak{g}_0$  zu den endlich vielen Unbestimmten von  $\mathfrak{G}_1^*$  führen wird.

$\mathfrak{m}$  besitzt nach § 3 als transformiertes Ideal mindestens ein in  $x_1$  reguläres Polynom  $C^{(1)}(x)$ , das etwa  $k$ -ter Dimension sei; also enthält  $\mathfrak{M}_0$  die Linearform  $C_{(x)}^{(1)} \xi_0$ . Wegen der Regularität von  $C^{(1)}(x)$  läßt jedes Polynom  $H(x)$  eine Darstellung zu:

$$(21) \quad H(x) \equiv b_0^{(2)} + b_1^{(2)} x_1 + \dots + b_{k-1}^{(2)} x_1^{k-1} (C^{(1)}(x));$$

so daß sich also, wegen der Zugehörigkeit von  $C_{(x)}^{(1)} \xi_0$  zu  $\mathfrak{M}_0$ , für  $\mathfrak{G}_0 | \mathfrak{M}_0$  tatsächlich ein Repräsentantensystem wählen läßt, das die  $k$ -te Dimension in  $x_1$  nicht erreicht.

Wird jetzt insbesondere für die Polynome  $G(x)$  aus  $\mathfrak{g}_1$  und  $F(x)$  aus  $\mathfrak{m}$  gesetzt:

$$(22) \quad \begin{cases} G(x) \equiv g_0^{(2)} + g_1^{(2)} x_1 + \dots + g_{k-1}^{(2)} x_1^{k-1} & (C^{(1)}(x)), \\ F(x) \equiv a_0^{(2)} + a_1^{(2)} x_1 + \dots + a_{k-1}^{(2)} x_1^{k-1} & (C^{(1)}(x)), \end{cases}$$

bedeutet ferner  $\mathfrak{G}_1^*$  das System aller Linearformen  $g(\xi) = g_0^{(2)} \xi_0 + \dots + g_{k-1}^{(2)} \xi_{k-1}$ , entsprechend  $\mathfrak{M}_1^*$  dasjenige der Linearformen  $a(\xi) = a_0^{(2)} \xi_0 + \dots + a_{k-1}^{(2)} \xi_{k-1}$ ; so folgt aus der Idealeigenschaft von  $\mathfrak{g}_1$  und  $\mathfrak{m}$ , daß  $\mathfrak{G}_1^*$  und  $\mathfrak{M}_1^*$  Moduln aus Linearformen in  $\xi_0 \dots \xi_{k-1}$  in bezug auf die ganzen Größen  $b^{(2)}, c^{(2)} \dots$  sind. Ebenso ergibt das aus  $C^{(1)}(x)$  abgeleitete Hauptideal einen Modul in bezug auf diese ganzen Größen:

$$\mathfrak{G}_1 = (\zeta_0, \zeta_1, \dots, \zeta_r, \dots),$$

wo  $\zeta_r = x_1^r C^{(1)}(x)$  gesetzt ist. Die  $\zeta_r$  sind linear unabhängig in bezug auf diese ganzen Größen  $b^{(2)}, c^{(2)}, \dots$ , und zwar sowohl unter sich wie von den endlich vielen  $\xi$ . Aus der Teilbarkeit von  $\mathfrak{G}_1$  durch  $\mathfrak{M}_1$  und folglich durch  $\mathfrak{G}_1^*$  folgt, daß auch  $\mathfrak{G}_1^*$  durch  $\mathfrak{G}_1$  bzw.  $\mathfrak{M}_1^*$  durch  $\mathfrak{M}_1$  teilbar ist. Unter Berücksichtigung von (22) kommt somit:

$$(23) \quad \mathfrak{G}_1 = (\mathfrak{G}_1^*, \mathfrak{G}_1); \quad \mathfrak{M}_1 = (\mathfrak{M}_1^*, \mathfrak{G}_1).$$

Aus (23) und der Linearunabhängigkeit der  $\xi$  und  $\zeta$  ergibt sich Satz VII für  $i = 2$  wie folgt. Wegen der Teilbarkeit von  $\mathfrak{G}_1$  durch  $\mathfrak{M}_1$  kommt vorerst:  $\mathfrak{G}_1 | \mathfrak{M}_1 = \mathfrak{G}_1^* | \mathfrak{M}_1$ . Um die Isomorphie mit  $\mathfrak{G}_1^* | \mathfrak{M}_1^*$  nachzuweisen, möge durch gewisse Linearformen  $g^*(\xi)$  aus  $\mathfrak{G}_1^*$  ein Repräsentantensystem von  $\mathfrak{G}_1^* | \mathfrak{M}_1^*$  gegeben sein. Wegen der Linearunabhängigkeit der  $\xi$  und  $\zeta$  folgt nun aus  $g^*(\xi) \equiv 0 (\mathfrak{M}_1)$  auch  $g^*(\xi) \equiv 0 (\mathfrak{M}_1^*)$ ; die  $g^*(\xi)$  sind somit auch modulo  $\mathfrak{M}_1$  inkongruent, bilden ein Repräsentantensystem von  $\mathfrak{G}_1^* | \mathfrak{M}_1$ ; und die durch dieses Repräsentantensystem vermittelte Zuordnung von  $\mathfrak{G}_1^* | \mathfrak{M}_1$  zu  $\mathfrak{G}_1^* | \mathfrak{M}_1^*$  ist isomorph nach Definition V.

Ganz entsprechend kommt:

Aus  $b^{(2)} g(\xi) \equiv 0 (\mathfrak{M}_1)$ ;  $b^{(2)} \neq 0$  folgt  $b^{(2)} g(\xi) \equiv 0 (\mathfrak{M}_1^*)$ ,  $b^{(2)} \neq 0$ .

Da dies für alle  $g(\xi)$  aus  $\mathfrak{G}_1^*$  und nur für diese erfüllt ist — denn  $\mathfrak{G}_1^*$  besteht nach (23) aus der Gesamtheit der Polynome des Grundideals  $\mathfrak{g}_1$ , die zugleich Linearformen in  $\xi$  sind — ist somit  $\mathfrak{G}_1^*$  als Grundmodul von  $\mathfrak{M}_1^*$  charakterisiert.

Adjungiert man schließlich  $x_3 \dots x_n$  zu  $P(u)$ , so kommt:

$$(24) \quad \left\{ \begin{array}{l} \mathfrak{G}_1^* = (\eta_1 \dots \eta_r); \quad \mathfrak{M}_1^* = (e_1 \eta_1, \dots, e_r \eta_r); \quad \mathfrak{G}_1 = (\eta_1 \dots \eta_r, \zeta_1 \dots \zeta_r \dots); \\ \mathfrak{M}_1 = (e_1 \eta_1, \dots, e_r \eta_r, \zeta_1 \dots \zeta_r \dots); \end{array} \right.$$

und somit:

$$(e_r) = \mathfrak{M}_1 / \mathfrak{G}_1 = \mathfrak{M}_1 / (\mathfrak{M}_1, \eta_r); \quad (e_{r-1}) = (\mathfrak{M}_1, \eta_r) / \mathfrak{G}_1 \text{ usw.}$$

womit unter Berücksichtigung von Anmerkung \*)  $e_r, e_{r-1}, \dots, e_1, 1, \dots, 1, \dots$  als Elementarteiler von  $\mathfrak{M}_1$  erkannt sind.

Damit ist für  $i = 2$  Satz VII in allen Teilen bewiesen.

Es sei bemerkt, daß (22) und (23) nur benutzen, daß  $C^{(1)}(x)$  in  $x_1$  regulär ist. Diese Formeln und die daran geknüpften, zu Satz VII führenden Überlegungen bleiben somit erhalten, wenn an Stelle von (12) die spezielle Transformation

$$(25) \quad y_1 = x_1; \quad y_2 = u_{21} x_1 + z_2; \quad \dots; \quad y_n = u_{n1} x_1 + z_n$$

zugrunde gelegt wird, die durch Zusammensetzen mit

$$(26) \quad \left\{ \begin{array}{l} z = U_1(x) \\ \text{oder} \\ z_2 = x_2; \quad z_3 = u_{32} x_2 + z_3; \quad \dots; \quad z_n = u_{n2} x_2 + \dots + u_{n, n-1} x_{n-1} + z_n \end{array} \right.$$

wieder (12) ergibt. Geht  $\tilde{m}_{(u)}$  vermöge (25) in  $\tilde{m}$  über und haben  $\tilde{g}_1, \tilde{\mathfrak{G}}_1 \dots$  die entsprechende Bedeutung für  $\tilde{m}$  wie  $g_1, \mathfrak{G}_1 \dots$  für  $m$ , so gilt also:

$$(27) \quad \tilde{\mathfrak{G}}_1 = (\tilde{\mathfrak{G}}_1^*, \tilde{\mathfrak{C}}_1); \quad \tilde{\mathfrak{M}}_1 = (\tilde{\mathfrak{M}}_1^*, \tilde{\mathfrak{C}}_1).$$

Dabei entsteht (27) aus (23) einfach vermöge der Umkehrung von (26). Denn dies ist offenbar erfüllt für  $m$  und  $C^{(1)}(x)$ , also auch für  $\mathfrak{G}_1$  und  $\mathfrak{M}_1$ . Es gilt aber auch für  $\mathfrak{g}_1$ , denn

$$b^{(2)}(x) G(x) \equiv 0(m), \quad b^{(2)} \neq 0 \quad \text{und} \quad \tilde{b}^{(2)}(z) \tilde{G}(x, z) \equiv 0(\tilde{m}), \quad \tilde{b}^{(2)} \neq 0$$

bedingen sich vermöge  $z = U_1(x)$  gegenseitig. Somit wird  $\tilde{\mathfrak{g}}_1 = \mathfrak{g}_1$  vermöge (26); also auch  $\tilde{\mathfrak{G}}_1 = \mathfrak{G}_1$ , und damit gilt nach der durch (22) gegebenen Definition für  $\mathfrak{G}_1^*$  und  $\mathfrak{M}_1^*$  das gleiche für  $\tilde{\mathfrak{G}}_1^*$  und  $\tilde{\mathfrak{M}}_1^*$  und somit für die ganze Darstellung (27).

Zum allgemeinen Induktionsschluß mögen die Voraussetzungen gelten:

$$,,(28) \quad \left\{ \begin{array}{l} \mathfrak{G}_{i-1} = (\mathfrak{G}_{i-1}^*, \mathfrak{G}_{i-1}), \quad \mathfrak{M}_{i-1} = (\mathfrak{M}_{i-1}^*, \mathfrak{G}_{i-1}), \\ \mathfrak{G}_{i-1} = (\xi_0, \xi_1, \dots, \xi_r, \dots), \end{array} \right.$$

wo  $\mathfrak{G}_{i-1}^*$  und  $\mathfrak{M}_{i-1}^*$  Moduln — in bezug auf die ganzen Größen  $b^{(i)}, c^{(i)}, \dots$  — aus Linearformen in endlich vielen Unbestimmten  $\xi$ , gewissen Potenzprodukten von  $x_1, \dots, x_{i-1}$ , bedeuten; und wo die  $\xi$  linear unabhängig sowohl unter sich wie von den  $\xi$  in bezug auf diese ganzen Größen seien. Eine (28) entsprechende Darstellung und die Linearunabhängigkeit der  $\xi$  und  $\zeta$  soll auch gelten, wenn statt (12) die spezielle Transformation

$$(29) \quad y_1 = x_1; \dots; y_{i-1} = u_{i-1,1}x_1 + \dots + x_{i-1};$$

$y_i = u_{i,1}x_1 + \dots + u_{i,i-1}x_{i-1} + z_i; \dots; y_n = u_{n,1}x_1 + \dots + u_{n,i-1}x_{i-1} + z_n$  zugrunde gelegt wird, die sich zu (12) zusammensetzen läßt vermöge

$$z = U_{i-1}(x) \quad \text{oder} \quad z_i = x_i; \quad z_{i+1} = u_{i+1,i}x_i + x_{i+1}; \dots;$$

$$z_n = u_{n,i}x_i + \dots + u_{n,n-1}x_{n-1} + x_n,$$

und zwar soll diese spezielle Darstellung aus (28) einfach durch Umkehrung von  $z = U_{i-1}(x)$  hervorgehen.

Aus den Voraussetzungen (28) und der Linearunabhängigkeit der  $\xi$  und  $\zeta$  folgt die Isomorphie von  $\mathfrak{G}_{i-1} | \mathfrak{M}_{i-1}$  mit  $\mathfrak{G}_{i-1}^* | \mathfrak{M}_{i-1}^*$ , vermöge Zuordnung zu dem gleichen Repräsentantensystem, durch genau die gleichen Überlegungen, die oben an (23) anknüpften; ebenso ergibt sich, daß  $\mathfrak{G}_{i-1}^*$  Grundmodul von  $\mathfrak{M}_{i-1}^*$  wird und daß  $\mathfrak{M}_{i-1}$  nur endlich viele von 1 verschiedene Elementarteiler besitzt, die von 1 verschiedenen Elementarteiler von  $\mathfrak{M}_{i-1}^*$ .

Zur Durchführung des Induktionsschlusses ist vorerst wieder zu zeigen, daß für  $\mathfrak{G}_{i-1} | \mathfrak{M}_{i-1}^*$ , also auch für  $\mathfrak{G}_{i-1} | \mathfrak{M}_{i-1}$ , ein in  $x_i$  beschränktes Repräsentantensystem genommen werden darf. Dies ergibt sich aus der in (7), Satz III bewiesenen Quotientendarstellung:

$$(30) \quad \mathfrak{G}_{i-1}^* = \mathfrak{M}_{i-1}^* / (C^{(i)}),$$

unter  $C^{(i)}$  irgendeine nicht identisch verschwindende Determinante  $\varrho$ -ten Grades aus  $\mathfrak{M}_{i-1}^*$  verstanden, wo  $\varrho$  den Rang von  $\mathfrak{M}_{i-1}^*$  bedeutet. Aus

dem auf die spezielle Transformation (29) bezüglichen Teil der Voraussetzungen ergibt sich, daß  $C^{(i)}$  *immer regulär in bezug auf  $x_i$  angenommen werden darf*. Danach hat nämlich der  $\mathfrak{M}_{i-1}^*$  entsprechende Modul  $\tilde{\mathfrak{M}}_{i-1}^*$  gleichen Rang; bedeutet somit  $\tilde{C}^{(i)}$  irgendeine nicht identisch verschwindende Determinante  $\varrho$ -ten Grades aus  $\tilde{\mathfrak{M}}_{i-1}^*$ , die durch  $z = U_{i-1}(x)$  in ein reguläres  $C^{(i)}$  übergeht, so wird nach der Voraussetzung  $C^{(i)}$  eine Determinante  $\varrho$ -ten Grades aus  $\mathfrak{M}_{i-1}^*$ .

Aus der Existenz von  $C^{(i)}$  folgt entsprechend (8), bei passender Nummerierung der  $\xi$ , die Zugehörigkeit von  $\varrho$  Linearformen der speziellen Gestalt

$$L_\lambda(\xi) = C^{(i)} \xi_\lambda + c_{\lambda,1}^{(i)} \xi_{\varrho+1} + \dots + c_{\lambda,s-\varrho}^{(i)} \xi_s \quad (\lambda = 1 \dots \varrho)$$

zu  $\mathfrak{M}_{i-1}^*$ . Nun kann jede Linearform in  $\xi$  auf die Form gebracht werden:

$$(31) \quad H(\xi) = a_1^{(i)} \xi_1 + \dots + a_\varrho^{(i)} \xi_\varrho + b_1^{(i)} \xi_{\varrho+1} + \dots + b_{s-\varrho}^{(i)} \xi_s \quad (L_1(\xi), \dots, L_\varrho(\xi)),$$

wo  $a_1^{(i)} \dots a_\varrho^{(i)}$  in  $x_i$  beschränkt sind, den Grad  $k$  von  $C^{(i)}$  nicht erreichen. Diese Darstellung ist *eindeutig*; denn aus

$$a_1^{(i)} \xi_1 + \dots + a_\varrho^{(i)} \xi_\varrho + b_1^{(i)} \xi_{\varrho+1} + \dots + b_{s-\varrho}^{(i)} \xi_s = 0 \quad (L_1(\xi), \dots, L_\varrho(\xi))$$

folgt durch Koeffizientenvergleichen in  $\xi_1 \dots \xi_\varrho$  unter Berücksichtigung der Grade in  $x_i$  das identische Verschwinden aller  $a^{(i)}$  und  $b^{(i)}$ .

Sei nun insbesondere

$$H(\xi) = 0 \quad (G_{i-1}^*); \text{ also } C^{(i)} H(\xi) = 0 \quad (\mathfrak{M}_{i-1}^*) \text{ nach (30).}$$

Daraus kommt wie beim Beweis von Satz III:  $C^{(i)} H(\xi) = 0 \quad (\mathfrak{M}_{i-1}^*)$

$$C^{(i)} H(\xi) = \sum_{\tau=1}^{s-\varrho} \{ C^{(i)} b_\tau^{(i)} - \sum_{\lambda} a_\lambda^{(i)} c_{\lambda,\tau}^{(i)} \} \xi_{\varrho+\tau} = 0 \quad (\mathfrak{M}_{i-1}^*)$$

und somit, da wie bei Satz III die Koeffizienten von  $\xi_{\varrho+1} \dots \xi_s$  verschwinden müssen:

$$C^{(i)} b_\tau^{(i)} = \sum_{\lambda} a_\lambda^{(i)} c_{\lambda,\tau}^{(i)}, \quad (\tau = 1 \dots s - \varrho),$$

woraus folgt, daß auch die  $b_\tau^{(i)}$  beschränkt sind, den Maximalgrad der  $c_{\lambda,\tau}^{(i)}$  nicht erreichen. Die Existenz eines in  $x_i$  beschränkten Repräsentantensystems für  $\mathfrak{G}_{i-1}^* | \mathfrak{M}_{i-1}^*$ , d. h. für  $\mathfrak{G}_{i-1} | \mathfrak{M}_{i-1}$ , das einen gewissen festen Grad  $r$  nicht erreicht, ist damit bewiesen.

Bezeichnet man jetzt mit  $\vartheta_1 \dots \vartheta_t$  die endlich vielen Potenzprodukte

$$\begin{aligned} x_i^\alpha \xi_\lambda & \quad (\alpha = 0, 1, \dots, k-1; \lambda = 1, 2, \dots, \varrho); \\ x_i^\beta \xi_{\varrho+\tau} & \quad (\beta = 0, 1, \dots, r-1; \tau = 1, 2, \dots, s-\varrho) \end{aligned}$$

und ordnet man die abzählbar unendlich vielen Ausdrücke

$$\begin{aligned} x_i^\gamma L_\lambda & \quad (\gamma = 0, 1 \dots \text{in inf.} \dots; \lambda = 1, 2, \dots, \varrho); \\ x_i^\gamma \xi_\tau & \quad (\gamma, \tau = 0, 1 \dots \text{in inf.} \dots) \end{aligned}$$



in eine einfach unendliche Reihe  $\omega_0, \omega_1, \dots, \omega_\mu, \dots$ , so sind die  $\theta$  und  $\omega$  linear unabhängig, sowohl einzeln unter sich wie voneinander, in bezug auf die ganzen Größen  $b^{(i+1)}, c^{(i+1)}, \dots$ . Denn aus

$$\sum c_{\alpha i}^{(i+1)} x_i^\alpha \xi_i + \sum c_{\beta i}^{(i+1)} x_i^\beta \xi_{i+1} + \dots + \sum d_{\gamma i}^{(i+1)} x_i^\gamma L_1(\xi) + \sum e_{\gamma i}^{(i+1)} x_i^\gamma \zeta_i = 0,$$

jede Summe erstreckt über endlich viele Glieder, folgt wegen der vorausgesetzten Linearunabhängigkeit der  $\xi$  und  $\zeta$ , und der  $\zeta$  unter sich in bezug auf die ganzen Größen  $b^{(i)}, \dots$ , das Verschwinden aller  $e_{\gamma i}^{(i+1)}$ . Aus der Eindutigkeit der Darstellung (31) ergibt sich weiter das Verschwinden der  $c_{\alpha i}^{(i+1)}$  und der  $c_{\beta i}^{(i+1)}$ , und daraus schließlich wegen der Linearunabhängigkeit der  $L_1(\xi)$  das Verschwinden der  $d_{\gamma i}^{(i+1)}$ .

Faßt man jetzt den Modul  $(\mathfrak{G}_{i-1}, L_1(\xi), \dots, L_\rho(\xi))$  auf als Modul  $\mathfrak{G}_i$  in bezug auf die ganzen Größen  $b^{(i+1)}$ , so wird  $\mathfrak{G}_i$  durch  $\mathfrak{M}_i$  teilbar, wegen der Teilbarkeit von  $\mathfrak{G}_{i-1}, L_1(\xi) \dots L_\rho(\xi)$  durch  $\mathfrak{M}_{i-1}$ , und es kommt

$$\mathfrak{G}_i = (\omega_0, \omega_1, \dots, \omega_\mu \dots).$$

Für jedes  $H(x) : : 0 \ (g_{i-1})$  gilt somit nach (28), (31) und dem oben Bewiesenen:

$$H(x) = b_1^{(i+1)} \theta_1 + \dots + b_i^{(i+1)} \theta_i(\mathfrak{G}_i) \left( \mathfrak{G}_i \right)$$

als Modulgleichung in bezug auf die ganzen Größen  $b^{(i+1)}, c^{(i+1)}$ . Nun ist aber  $g_i$  durch  $g_{i-1}$  teilbar,  $m$  teilbar durch  $g_i$ ; wird somit insbesondere für jedes  $G(x)$  aus  $\mathfrak{G}_i$  und jedes  $F(x)$  aus  $\mathfrak{M}_i$  gesetzt:

$$G(x) = g^{(i+1)} \theta_1 + \dots + g_i^{(i+1)} \theta_i(\mathfrak{G}_i)$$

$$F(x) = a^{(i+1)} \theta_1 + \dots + a^{(i+1)} \theta_i(\mathfrak{G}_i)$$

und wird der aus allen  $g(\theta)$  bestehende Modul mit  $\mathfrak{G}_i^*$ , der aus allen  $a(\theta)$  bestehende mit  $\mathfrak{M}_i^*$  bezeichnet, so kommt durch genau die Überlegungen, die zu (23) führten:

$$(32) \quad \mathfrak{G}_i = (\mathfrak{G}_i^*, \mathfrak{G}_i); \quad \mathfrak{M}_i = (\mathfrak{M}_i^*, \mathfrak{G}_i); \quad \mathfrak{G}_i = (\omega_0, \omega_1, \dots, \omega_\mu \dots).$$

Dabei war bei der Herleitung von (32) wieder nur die Regularität von  $C^{(i)}$  in  $x_i$  benutzt, die ganze Überlegung bleibt also erhalten, wenn die spezielle Transformation (29) für einen Index höher zugrunde gelegt wird. Dabei zeigen genau die gleichen Überlegungen, die an (27) anknüpften, daß diese spezielle Darstellung aus (32) einfach durch die Umkehrung von  $z = U_i(x)$  hervorgeht.

Dadurch sind alle Voraussetzungen (28) usw. des allgemeinen Induktionsschlusses für einen Index höher bewiesen, und da aus diesen Voraussetzungen, wie dort gezeigt ist, unmittelbar Satz VII folgt, ist Satz VII somit allgemein bewiesen. Damit ist zugleich gezeigt, daß die durch

die Willkürlichkeit der  $C^{(4)}$  gegebene Willkür der  $\mathfrak{G}_{i-1}^*$ ,  $\mathfrak{M}_{i-1}^*$  durch die Isomorphie des Restklassensystems  $\mathfrak{G}_{i-1}^*$ ,  $\mathfrak{M}_{i-1}^*$  wieder aufgehoben wird.

Ist insbesondere der in § 3 als Koeffizientenbereich zugrunde gelegte Körper  $P$  von der Charakteristik Null — d. h. ist der in  $P$  enthaltene, aus der Einheit abgeleitete Primkörper vom Typus der rationalen Zahlen —, so lassen sich die Unbestimmten  $u_{\mu}$  so zu Größen  $\bar{u}_{\mu}$  aus  $P$  spezialisieren, daß für  $i = 1 \dots n$  jeweils  $C^{(4)}$  regulär in  $x_i$  bleibt. Die obigen Überlegungen zeigen, daß Satz VII auch bei dieser Spezialisierung erhalten bleibt<sup>14)</sup>. Grundmodul und Elementarteiler brauchen dabei aber nicht notwendig durch die Spezialisierung  $u_{\mu} = \bar{u}_{\mu}$  aus dem allgemeinen Fall hervorzugehen<sup>15)</sup>.

## § 5.

### Resultantenform und Elementarteilerform eines Ideals aus Polynomen.

Es seien  $x_{i+1} \dots x_n$  zu  $P(u)$  adjungiert, so daß also  $\mathfrak{G}_{i-1}$  und  $\mathfrak{M}_{i-1}$  und folglich auch  $\mathfrak{G}_{i-1}^*$  und  $\mathfrak{M}_{i-1}^*$  in Linearformenmoduln übergehen, wo die ganzen Größen sich als Polynome einer Unbestimmten  $x_i$  auffassen lassen. Nach Satz VII stimmen in diesem Fall die von 1 verschiedenen Elementarteiler von  $\mathfrak{M}_{i-1}$ , und höchstens endlich viele Elementarteiler 1 von  $\mathfrak{M}_{i-1}$  mit denen von  $\mathfrak{M}_{i-1}^*$  überein. Das Produkt dieser Elementarteiler, der  $q$ -te Determinantenteiler von  $\mathfrak{M}_{i-1}^*$ , war gleich der Determinante der Übergangssubstitution von  $\mathfrak{G}_{i-1}^*$  nach  $\mathfrak{M}_{i-1}^*$ , also gleich  $N(\mathfrak{G}_{i-1}^* | \mathfrak{M}_{i-1}^*)$  nach Definition III. Nach (24) bzw. der aus (28) sich ergebenden analogen Formel für allgemeines  $i$  zeigt sich, daß das Produkt dieser Elementarteiler auch gleich der Determinante der Übergangs-

<sup>14)</sup> Hentzelt nimmt statt eines beliebigen  $P$  nur den Körper aller komplexen Zahlen und betrachtet hauptsächlich diesen letzteren Fall, während er nur bei der eigentlichen Eliminationstheorie Unbestimmte zugrunde legt. Hentzelt zeigt dann weiter, und zwar wesentlich mit den hier gegebenen Schlüssen, daß es zur Bildung der Resultantenform genügt, jeweils in  $\mathfrak{M}_{i-1}$  bis zu irgendeinem endlichen, eine feste Grenze überschreitenden Grad in den  $x$  zu gehen. Es fehlt aber die in Satz VII gegebene Isomorphie von  $\mathfrak{G}_{i-1} | \mathfrak{M}_{i-1}$  mit  $\mathfrak{G}_{i-1}^* | \mathfrak{M}_{i-1}^*$ , die den Grund für diese Unabhängigkeit von den Gradzahlen darlegt. (E. N.)

<sup>15)</sup> Für  $m = (x^2, ux + y)$  kommt  $g_0 = (1)$ ,  $g_1 = (1)^{\vee}$ . Wählt man  $C^{(1)} = x^2$ , so wird  $\mathfrak{G}_1^* = (1, x)$ ;  $\mathfrak{M}_1^* = (ux + y, xy)$ , wobei  $\mathfrak{M}_1^*$  die Elementarteiler  $y^2$  und 1 besitzt und  $C^{(2)} = y^2$  gewählt werden kann. Für  $u = 0$  bleiben  $C^{(1)}$  und  $C^{(2)}$  regulär in  $x$  bzw.  $y$ ; aber  $\mathfrak{M}_1^* = (y, xy)$  besitzt die Elementarteiler  $y, y$ . Es wird also auch  $\mathfrak{G}_1 | \mathfrak{M}_1$  dem Restklassensystem eines endlichen Moduls isomorph, aber nicht isomorph zu  $\mathfrak{G}_1 | \mathfrak{M}_1$ . Hätte man dagegen  $C^{(1)} = ux + y$  gewählt und so spezialisiert, daß  $C^{(1)}$  regulär geblieben wäre, so wäre auch die Isomorphie erhalten geblieben. (E. N.)

substitution von  $\mathfrak{G}_{i-1}$  nach  $\mathfrak{M}_{i-1}$  wird, also mit  $N(\mathfrak{G}_{i-1} \cdot \mathfrak{M}_{i-1})$  zu bezeichnen ist. Es kommt also

$$N(\mathfrak{G}_{i-1} | \mathfrak{M}_{i-1}) = N(\mathfrak{G}_{i-1}^* | \mathfrak{M}_{i-1}^*) = R^{(i)}(x),$$

wo das Polynom  $R^{(i)}(x)$ , also der größte gemeinsame Teiler im Polynomsinne aller  $\varrho$ -reihigen Determinanten aus  $\mathfrak{M}_{i-1}^*$ , als ganz und primitiv in  $x_{i+1} \dots x_n$  angenommen werden darf und folglich als Teiler von  $C^{(i)}$  regulär in  $x_i$  wird. Ebenso darf der höchste Elementarteiler  $E^{(i)}(x)$  von  $\mathfrak{M}_{i-1}$  bzw.  $\mathfrak{M}_{i-1}^*$  als ganz und primitiv in  $x_{i+1} \dots x_n$  und folglich als regulär in  $x_i$  angenommen werden. Dies führt zu

**Definition VI.** Das Polynom  $R^{(i)}(x)$  wird als Resultante  $i$ -ter Stufe von  $m$  bezeichnet;  $E^{(i)}(x)$  als Elementarteiler  $i$ -ter Stufe. Die Resultante  $i$ -ter Stufe wird also die Norm des Grundideals  $\mathfrak{g}_{i-1}$  nach  $m$ , aufgefaßt als Norm des Moduls  $\mathfrak{G}_{i-1}$  nach  $\mathfrak{M}_{i-1}$ , wobei  $x_{i+1} \dots x_n$  zu  $P(u)$  adjungiert sind; ebenso wird  $(E^{(i)}(x))$  bei derselben Adjunktion gleich dem Quotienten  $\mathfrak{M}_{i-1} / \mathfrak{G}_{i-1}$ . Als Resultantenform bzw. Elementarteilerform von  $m$  werden die Produkte

$$R_m = R^{(1)} \cdot R^{(2)} \cdot \dots \cdot R^{(n)}; \quad E_m = E^{(1)} \cdot E^{(2)} \cdot \dots \cdot E^{(n)}$$

bezeichnet.

Für Resultanten- und Elementarteilerform gilt

**Satz VIII.** Die Resultantenform ist durch die Elementarform teilbar; umgekehrt ist eine Potenz von  $E_m$  durch  $R_m$  teilbar.  $E_m$  und  $R_m$  sind durch  $m$  teilbar; allgemeiner wird  $E^{(i)} \dots E^{(n)} \mathfrak{g}_{i-1} = 0(m)$  und folglich  $R^{(i)} \dots R^{(n)} \mathfrak{g}_{i-1} = 0(m)$ .

Da nämlich die Norm durch den höchsten Elementarteiler teilbar ist und umgekehrt eine Potenz dieses höchsten Elementarteilers durch die Norm teilbar ist, folgt diese Teilbarkeit für  $R^{(i)}(x)$  und  $E^{(i)}(x)$  bei Adjunktion von  $x_{i+1} \dots x_n$ . Da aber  $R^{(i)}(x)$  und  $E^{(i)}(x)$  als primitive Polynome in bezug auf  $x_{i+1} \dots x_n$  vorausgesetzt sind, gilt die Teilbarkeit in bezug auf alle Unbestimmten  $x_i, x_{i+1}, \dots, x_n$ , und somit gilt die Teilbarkeit von  $R_m$  durch  $E_m$  und einer Potenz von  $E_m$  durch  $R_m$  nach der Definition dieser Ausdrücke in bezug auf alle Unbestimmten  $x$ .

Der höchste Elementarteiler  $E^{(i)}(x)$  ist ferner nach Satz VII und Satz II, bei Adjunktion von  $x_{i+1} \dots x_n$ , definiert als Quotient  $\mathfrak{M}_{i-1} / \mathfrak{G}_{i-1}$ . Folglich gibt es, wenn man wieder zu Polynomen in allen Unbestimmten  $x$  zurückgeht, zu jedem

$$(33) \quad G(x) \equiv 0(\mathfrak{g}_{i-1}) \text{ ein } b^{(i+1)} \neq 0, \text{ so daß } b^{(i+1)} E^{(i)}(x) G(x) \equiv 0(m)$$

wird. Nun wird insbesondere  $\mathfrak{g}_0$  gleich dem Einheitsideal, also kommt:

$$b^{(1)} E^{(1)}(x) \equiv 0(m); \quad b^{(2)} \neq 0 \quad \text{und somit} \quad E^{(1)}(x) \equiv 0(\mathfrak{g}_1).$$

Allgemein gibt es nach (33) zu

$E^{(1)}(x) \dots E^{(i-1)}(x) = 0(g_{i-1})$  ein  $b^{(i+1)} \neq 0$ , so daß  $b^{(i+1)} E^{(1)} \dots E^{(i)} = 0(m)$ ; also  $E^{(1)} \dots E^{(i)} = 0(g_i)$  wird. Wegen  $g_n = m$  ergibt sich also

$$(34) \quad E_m = E^{(1)} \dots E^{(n)} \equiv 0(m) \text{ und folglich } R_m = R^{(1)} \dots R^{(n)} \equiv 0(m).$$

Läßt man  $G(x)$  in (33) die endlich vielen Polynome einer Idealbasis von  $g_{i-1}$  durchlaufen und bedeutet  $c^{(i+1)}(x)$  das Produkt der diesen entsprechenden  $b^{(i+1)}(x)$ , so kommt

$$c^{(i+1)} E^{(i)}(x) g_{i-1} \equiv 0(m); \quad c^{(i+1)} \neq 0 \quad \text{und also} \quad E^{(i)}(x) g_{i-1} \equiv 0(g_i)$$

und daraus wie oben durch endlich oftmalige Wiederholung:

$$E^{(n)}(x) \dots E^{(i)}(x) g_{i-1} \equiv 0(m)$$

und folglich auch  $R^{(n)}(x) \dots R^{(i)}(x) g_{i-1} \equiv 0(m)$ ,

womit Satz VIII in allen Teilen bewiesen ist.

Satz VIII beruht wesentlich auf Eigenschaften der Elementarteilerform; daß aber die *Resultantenform eine charakteristische Bedeutung* für  $m$  hat, zeigt

Satz IX. *Ist  $n$  ein Teiler von  $m$  — Teiler im Idealsinn verstanden — und stimmen die Resultantenformen  $R_n$  und  $R_m$  überein, so stimmen die Ideale  $n$  und  $m$  überein.*

Bedeutet nämlich  $g_0 \dots g_{n-1}$ ,  $g_n = m$  und  $h_0 \dots h_{n-1}$ ,  $h_n = n$  die Grundideale von  $m$  und  $n$ , so werden vorerst  $g_0$  und  $h_0$  gleich dem Einheitsideal, also  $g_0 = h_0$ . Setzt man jetzt  $g_{i-1} = h_{i-1}$  voraus, so daß also  $\mathfrak{M}_{i-1}$  und  $\mathfrak{N}_{i-1}$  beide denselben Grundmodul  $\mathfrak{G}_{i-1}$  besitzen, so läßt die Voraussetzung  $R_n = R_m$  bei Adjunktion von  $x_{i+1} \dots x_n$  die Fassung zu:

$$N(\mathfrak{G}_{i-1} | \mathfrak{N}_{i-1}) = N(\mathfrak{G}_{i-1} | \mathfrak{M}_{i-1}) \text{ oder auch } N(\mathfrak{G}_{i-1}^* | \mathfrak{N}_{i-1}^*) = N(\mathfrak{G}_{i-1}^* | \mathfrak{M}_{i-1}^*),$$

dabei ist entsprechend (32) gesetzt:  $\mathfrak{N}_{i-1} = (\mathfrak{N}_{i-1}^*, \mathfrak{G}_{i-1})$ , so daß  $\mathfrak{N}_{i-1}^*$  also auch ein Linearformenmodul in  $\xi$  wird und  $\mathfrak{G}_{i-1}^*$  sein Grundmodul. Wegen der Teilbarkeit von  $\mathfrak{M}_{i-1}$  durch  $\mathfrak{N}_{i-1}$ , die die Teilbarkeit von  $\mathfrak{M}_{i-1}^*$  durch  $\mathfrak{N}_{i-1}^*$  nach sich zieht, folgt daraus nach Satz IV, daß bei dieser Adjunktion die beiden Moduln  $\mathfrak{N}_{i-1}^*$  und  $\mathfrak{M}_{i-1}^*$  und folglich auch  $\mathfrak{N}_{i-1}$  und  $\mathfrak{M}_{i-1}$  übereinstimmen. Die Adjunktion von  $x_{i+1} \dots x_n$  bedeutet aber, daß zu  $\mathfrak{M}_{i-1}$  bzw.  $m$  noch alle solche Polynome  $G(x)$  hinzugefügt werden, für die

$$b^{(i+1)}(x) G(x) \equiv 0(m); \quad b^{(i+1)} \neq 0$$

wird, d. h. durch die Adjunktion geht  $\mathfrak{M}_{i-1}$  bzw.  $m$  in  $g_i$ , entsprechend  $n$  in  $h_i$  über; somit ist  $g_i = h_i$  und folglich  $g_n = h_n$ , also  $m = n$  bewiesen.

Schließlich ergibt dasselbe Übertragungsprinzip, angewandt auf Satz V, noch

**Satz X.** *Es sei  $R^{(i)} = S^{(i)} T^{(i)}$  eine Zerlegung von  $R^{(i)}$  in — im Polynomsinn — teilerfremde Polynome  $S^{(i)}$  und  $T^{(i)}$ . Dann existiert ein und nur ein Ideal  $\mathfrak{j}$ , ebenso ein und nur ein Ideal  $\mathfrak{t}$ , die beide Teiler von  $\mathfrak{m}$  mit gleichem Grundideal  $(i-1)$ -ter Stufe  $\mathfrak{g}_{i-1}$  sind, derart daß  $S^{(i)}$  gleich  $N(\mathfrak{G}_{i-1} | \mathfrak{S}_{i-1})$ ,  $T^{(i)}$  gleich  $N(\mathfrak{G}_{i-1} | \mathfrak{T}_{i-1})$  wird.  $\mathfrak{j}$  und  $\mathfrak{t}$  sind definiert als Gesamtheit der Polynome  $S(x)$  bzw.  $T(x)$  derart, daß*

$$s^{(i+1)}(x) T^{(i)}(x) S(x) \equiv 0 \pmod{\mathfrak{m}}; \quad s^{(i+1)} \neq 0$$

$$t^{(i+1)}(x) S^{(i)}(x) T(x) \equiv 0 \pmod{\mathfrak{m}}; \quad t^{(i+1)} \neq 0$$

wird und es wird  $\mathfrak{g}_i$  gleich dem kleinsten Vielfachen von  $\mathfrak{j}$  und  $\mathfrak{t}$ ,

$$\mathfrak{g}_i = [\mathfrak{j}, \mathfrak{t}].$$

Dazu ist nur zu bemerken, daß  $s^{(i+1)}, t^{(i+1)}$  für  $\mathfrak{j}$  und  $\mathfrak{t}$  fest gewählt werden können, als Produkt der den Basiselementen von  $\mathfrak{j}$  bzw.  $\mathfrak{t}$  entsprechenden  $s^{(i+1)}, t^{(i+1)}$ , und daß, wie oben bemerkt, bei Adjunktion von  $x_{i+1} \dots x_n$  sich  $\mathfrak{m}$  in  $\mathfrak{g}_i$  verwandelt. Insbesondere läßt sich die Zerlegung von  $R^{(i)}$  bis auf Potenzen irreduzibler Polynome — primäre Faktoren — fortsetzen, was eine entsprechende Darstellung für  $\mathfrak{g}_i$  als kleinstes gemeinsames Vielfaches nach sich zieht.

## § 6.

### Eigentliche Eliminationstheorie.

Nach Satz VIII bzw. Formel (34) sind *Resultanten- und Elementarteilerform* durch  $\mathfrak{m}$  teilbar, verschwinden also für alle Nullstellen von  $\mathfrak{m}$ ; dabei sind unter „Nullstellen von  $\mathfrak{m}$ “ solche — dem aus  $P(u; x_{i+1} \dots x_n)$  abgeleiteten algebraisch-abgeschlossenen Körper angehörigen<sup>10)</sup> — Wertsysteme von  $x_1 \dots x_i$  verstanden, daß für diese Wertsysteme jedes Polynom aus  $\mathfrak{m}$  verschwindet, wobei man sich  $x_{i+1} \dots x_n$  dem Koeffizientenbereich adjungiert denkt ( $i = 1, \dots, n$ ). Diese adjungierten  $x_{i+1} \dots x_n$  können, wie gezeigt werden wird, auch durch Größen aus  $P(u)$  ersetzt werden. *Inhalt der Eliminationstheorie ist umgekehrt die Ableitung der Nullstellen von  $\mathfrak{m}$  aus denjenigen der Resultantenform.* Diese Umkehrung beruht auf der in diesem Paragraphen zu entwickelnden *sukzessiven Elimination*; indem im

<sup>10)</sup> Daß jeder Körper, und zwar im wesentlichen eindeutig, sich zu einem algebraisch-abgeschlossenen erweitern läßt, hat Steinitz in seiner Algebraischen Theorie der Körper (J. f. M. 137 (1910), S. 167–309) gezeigt und damit das rationale Äquivalent für den Fundamentalsatz der Algebra gegeben. Tatsächlich handelt es sich jeweils für  $i = 1, \dots, n$  um einen endlichen Erweiterungskörper von  $P(u, x_{i+1}, \dots, x_n)$ . (E. N.)

nächsten Paragraphen die Teilbarkeit der dabei auftretenden Form  $D^{(i)}(x)$  durch  $E^{(i)}(x)$  nachgewiesen wird, folgt aus der Teilbarkeit einer Potenz von  $E^{(i)}(x)$  durch  $R^{(i)}(x)$  die gewünschte Umkehrung.

Die hier zu gebende Theorie der sukzessiven Elimination beruht auf

**Satz XI.** *Es bedeute  $\mathfrak{b}$  ein Ideal aus Polynomen in einer Unbestimmten  $t$  mit Koeffizienten aus  $P$ , also ein Hauptideal;  $h(t)$  ein Polynom aus  $\mathfrak{b}$  vom Grade  $k$ ,  $\mathfrak{B}$  den Linearformenmodul in  $1, t, \dots, t^{k-1}$ , in den  $\mathfrak{b}$  modulo  $h(t)$  übergeht. Dann ist  $\mathfrak{B}$  vom Range  $k - p$ , wenn  $p$  den Grad des Basispolynoms  $f(t)$  von  $\mathfrak{b}$  bedeutet.*

Nach Voraussetzung wird  $h(t) = h_1(t) \cdot f(t)$ , wo  $h_1(t)$  vom Grade  $k - p$  ist. Die durch die Polynome  $f(t), t f(t), \dots, t^{k-p-1} f(t)$  repräsentierten Restklassen von  $\mathfrak{b}$  nach  $h(t)$  sind also linear unabhängig; und jede Restklasse von  $\mathfrak{b}$  nach  $h(t)$  läßt sich linear, mit Koeffizienten aus  $P$ , durch diese  $k - p$  speziellen darstellen.  $\mathfrak{b}$  geht aber modulo  $h(t)$  in einen Linearformenmodul in  $1, t, \dots, t^{k-1}$  über, dessen Rang somit genau  $k - p$  ist.

Sei jetzt  $\alpha = \alpha_1$  ein transformiertes Ideal aus Polynomen,  $A^{(1)}(x)$  ein in  $x_1$  reguläres Polynom aus  $\alpha_1$  vom Grade  $k_1$ ; und  $\mathfrak{U}_1$  der Linearformenmodul in  $1, x_1, \dots, x_1^{k_1-1}$ , mit Polynomen  $a^{(2)}(x)$  als Koeffizienten, in den  $\alpha_1$  modulo  $A^{(1)}(x)$  übergeht. Es bedeute ferner  $\alpha_2$  das aus allen  $k_1$ -reihigen Determinanten aus  $\mathfrak{U}_1$  abgeleitete Ideal in  $x_2 \dots x_n$ . Nach Satz XI ist  $\alpha_2$  dann und nur dann gleich dem Nullideal, wenn die Polynome aus  $\alpha_1$  einen gemeinsamen Teiler — Teiler im Polynomsinn verstanden — vom Grade  $p_1 > 0$  in  $x_1$  besitzen. Ist  $\alpha_2$  vom Nullideal verschieden, so enthält es, da  $\alpha$  als transformiertes Ideal vorausgesetzt war, ein in  $x_2$  reguläres Polynom  $A^{(2)}(x)$  vom Grade  $k_2$ , wie man durch Zusammensetzen der Transformation (12) aus den speziellen Transformationen (25) und (26) direkt sieht. Es bedeute wieder  $\mathfrak{U}_2$  den Linearformenmodul in  $1, x_2, \dots, x_2^{k_2-1}$ , in den  $\alpha_2$  modulo  $A^{(2)}(x)$  übergeht,  $\alpha_3$  das aus allen  $k_2$ -reihigen Determinanten aus  $\mathfrak{U}_2$  abgeleitete Ideal in  $x_3 \dots x_n$ , das ein in  $x_3$  reguläres Polynom  $A^{(3)}(x)$  enthalten muß.

Auf diese Art setze man das Verfahren fort, bis man zu einem Nullideal kommt oder bis  $\alpha_{n+1}$  gleich dem Einheitsideal wird; denn da  $\alpha_{n+1}$  von den  $x$  frei ist, kann es nur das Nullideal oder Einheitsideal sein. Es zeigt sich, daß die Ideale  $\alpha_1, \alpha_2, \dots$  eindeutig durch  $\alpha$  bestimmt sind, unabhängig von den zugrunde gelegten Polynomen  $A^{(i)}(x)$ . Das ist klar für  $\alpha_1 = \alpha$ , kann also für  $\alpha_1, \dots, \alpha_i$  vorausgesetzt werden. Geht jetzt  $\alpha_i$  modulo  $A^{(i)}(x)$  über in den Linearformenmodul  $\mathfrak{U}_i$ , so läßt sich  $\mathfrak{U}_i$  auch charakterisieren als Gesamtheit der Polynome aus  $\alpha_i$ , die in  $x_i$  den Grad  $k_i$  nicht erreichen;  $\mathfrak{U}_i$  hängt also nur vom Grade  $k_i$  von  $A^{(i)}(x)$  ab. Sei

jetzt  $A^{(i)}(x)$  vom Grade  $k_i > k_i$  ein in  $x_i$  reguläres Polynom aus  $\mathfrak{a}_i$ ,  $\mathfrak{A}_i$  der entsprechende Linearformenmodul,  $\bar{\mathfrak{a}}_{i+1}$  das aus den  $\bar{k}_i$ -reihigen Determinanten aus  $\bar{\mathfrak{A}}_i$  abgeleitete Ideal. Dann gilt die Modulgleichung

$$\bar{\mathfrak{A}}_i = (\mathfrak{A}_i, A^{(i)}, x_i A^{(i)}, \dots, x_i^{\bar{k}_i - k_i - 1} A^{(i)}).$$

Da nun wegen der Regularität von  $A^{(i)}(x)$  in  $x_i$  sich die Polynome  $A^{(i)}, x_i A^{(i)}, \dots$  als neue Unbestimmte der Linearformen einführen lassen, folgt daraus das Übereinstimmen der  $k_i$ -reihigen Determinanten aus  $\mathfrak{A}_i$  mit den  $\bar{k}_i$ -reihigen aus  $\mathfrak{A}_i$ ; und somit kommt  $\bar{\mathfrak{a}}_{i+1} = \mathfrak{a}_{i+1}$ .<sup>17)</sup>

Es ist ferner stets  $\mathfrak{a}_{i+1}$  durch  $\mathfrak{a}_i$  teilbar. Das ist klar, wenn  $\mathfrak{a}_{i+1}$  das Nullideal ist; im entgegengesetzten Fall ist  $\mathfrak{A}_i$  vom Range  $k_i$ ; also ist  $\mathfrak{a}_{i+1}$ , das nach Definition aus den  $k_i$ -reihigen Determinanten aus  $\mathfrak{A}_i$  besteht, durch  $\mathfrak{A}_i$  und folglich durch  $\mathfrak{a}_i$  teilbar. Jedes  $\mathfrak{a}_{i+1}$  ist somit durch  $\mathfrak{a}$  teilbar; wird also  $\mathfrak{a}_{n+1}$  gleich dem Einheitsideal, so ist auch  $\mathfrak{a}$  gleich dem Einheitsideal.

Es sei jetzt  $\mathfrak{a}$  vom Einheitsideal verschieden;  $\mathfrak{a}_1 \neq 0, \dots, \mathfrak{a}_i \neq 0$ ;  $\mathfrak{a}_{i+1} = 0$ .  $D^{(i)}(x)$  sei der nach Satz XI existierende größte gemeinsame Teiler — Teiler im Polynomsinn verstanden — aller Polynome aus  $\mathfrak{a}_i$ ; als Teiler von  $A^{(i)}(x)$  wird  $D^{(i)}(x)$  selbst regulär in  $x_i$  vom Grade  $p_i > 0$ . Man adjungiere  $x_{i+1} \dots x_n$  zu  $P(u)$ ; dann läßt  $D^{(i)}(x)$  in einem algebraischen Erweiterungskörper von  $P(u; x_{i+1} \dots x_n)$  eine Zerlegung in  $p_i$  Linearfaktoren zu. Sei  $x_i - \bar{x}_i$  ein solcher Linearfaktor, so daß für  $x_i = \bar{x}_i$  alle Polynome aus  $\mathfrak{a}_i$  verschwinden und daß folglich nach Satz XI die Polynome aus  $\mathfrak{a}_{i-1}$  für diese Spezialisierung einen größten gemeinsamen Teiler  $D^{(i-1)}(x)$  erhalten. Als Teiler von  $A^{(i-1)}(x)$  wird  $D^{(i-1)}(x)$  selbst wieder regulär in  $x_{i-1}$  vom Grade  $p_{i-1} > 0$ ; kann also insbesondere nicht identisch verschwinden und läßt in einem Erweiterungskörper von  $P(u, \bar{x}_i, x_{i+1}, \dots, x_n)$  eine Zerlegung in  $p_{i-1}$  Linearfaktoren zu. Ist  $x_{i-1} - \bar{x}_{i-1}$  ein solcher Linearfaktor, so entspricht diesem ein größter gemeinsamer Teiler aus  $\mathfrak{a}_{i-2}$ . So fortfahrend gelangt man zu endlich vielen gemeinsamen Nullstellen von  $\mathfrak{a}$ , die in einem algebraischen Erweiterungskörper von  $P(u; x_{i+1} \dots x_n)$  liegen. Umgekehrt ist wegen der Teilbarkeit von  $\mathfrak{a}_i$  durch  $\mathfrak{a}$  jede Nullstelle von  $\mathfrak{a}$  auch eine solche von  $\mathfrak{a}_i$ . Ist also insbesondere  $x_1 = \bar{x}_1, \dots, x_i = \bar{x}_i, x_{i+1} = x_{i+1}, \dots, x_n = x_n$  Nullstelle von  $\mathfrak{a}$ , so folgt daraus  $\mathfrak{a}_{i+1} = 0$ ; und die Polynome aus  $\mathfrak{a}_i$  erhalten einen größten gemeinsamen Teiler mit dem Linearfaktor  $x_i - \bar{x}_i$ . Zusammenfassend kommt:

Satz XII. Sei  $\mathfrak{a}$  vom Einheitsideal verschieden,  $\mathfrak{a}_1 \neq 0, \dots, \mathfrak{a}_i \neq 0$ ;  $\mathfrak{a}_{i+1} = 0$ , dann existieren bei Adjunktion von  $x_{i+1} \dots x_n$  zu  $P(u)$

<sup>17)</sup> Es ist das im Prinzip derselbe Schluß, auf dem die Isomorphie von  $\mathfrak{G}_{i-1}^* | \mathfrak{M}_{i-1}^*$ , mit  $\mathfrak{G}_{i-1} | \mathfrak{M}_{i-1}$  beruhte.

endlich viele zusammengehörige Wertsysteme  $\bar{x}_1 \dots \bar{x}_i$ , die in einem algebraischen Erweiterungskörper von  $P(u, x_{i+1}, \dots, x_n)$  liegen, derart, daß alle Polynome aus  $\alpha$  für  $x_1 = \bar{x}_1, \dots, x_i = \bar{x}_i, x_{i+1} = x_{i+1}, \dots, x_n = x_n$  verschwinden. Liegt umgekehrt eine solche Nullstelle von  $\alpha$  vor, so folgt daraus  $\alpha_{i+1} = 0$ , und das Auftreten eines gemeinsamen Teilers  $D^{(i)}(x)$  aller Polynome aus  $\alpha$ , der den Linearfaktor  $x_i - \bar{x}_i$  besitzt.

Satz XII zeigt insbesondere, daß jedes Ideal  $\alpha$ , das keine Nullstelle besitzt, gleich dem Einheitsideal wird.

Um eine Zerlegung durchzuführen, welche die Zusammengehörigkeit der Wertsysteme auch explizit zeigt, führt man neue Unbestimmte  $v$  ein, die  $P(u, x_{i+1}, \dots, x_n)$  adjungiert werden mögen. Sei gesetzt:

$$(35) \quad x_i = -v_1 x_1 - \dots - v_{i-1} x_{i-1} + z_i,$$

so daß die Zusammensetzung von (12) mit (35) wieder eine Substitution vom Typus (12) ergibt, wo jetzt nur die  $u_{i,\kappa}$  ersetzt sind durch  $w_{i,\kappa} = u_{i,\kappa} - v_\kappa$ , und allgemeiner  $u_{i+\lambda,\kappa}$  durch  $w_{i+\lambda,\kappa} = u_{i+\lambda,\kappa} - u_{i+\lambda,i} v_\kappa$ . Führt somit die Substitution (35) das nach Voraussetzung transformierte Ideal  $\alpha$  über in  $\mathfrak{b}$ , so entsteht  $\mathfrak{b}$  einfach aus  $\alpha$  durch Ersetzen der  $u_\mu$  durch  $w_\mu$ , und Adjunktion der  $v$ ; und durch den gleichen Prozeß entstehen die vermöge  $\mathfrak{b}$  definierten Ideale  $\mathfrak{b}_1, \mathfrak{b}_2, \dots$  aus  $\alpha_1, \alpha_2, \dots$ . Umgekehrt geht  $\alpha_1$  aus  $\mathfrak{b}_1$  vermöge  $v = 0$  hervor; die Ideale  $\alpha_2$  und  $\mathfrak{b}_2$  sind also gleichzeitig Nullideale, oder gleichzeitig vom Nullideal verschieden.

Sei jetzt wieder  $\alpha_1 \neq 0; \dots; \alpha_i \neq 0; \alpha_{i+1} = 0$ ; also auch  $\mathfrak{b}_1 \neq 0; \dots; \mathfrak{b}_i \neq 0; \mathfrak{b}_{i+1} = 0$ ; sei  $\bar{x}_1 \dots \bar{x}_i, x_{i+1} \dots x_n$  ein zusammengehöriges Nullstellensystem von  $\alpha$ . Definiert man  $\bar{z}_i = \bar{x}_i + v_1 \bar{x}_1 + \dots + v_{i-1} \bar{x}_{i-1}$ , so wird  $\bar{x}_1 \dots \bar{x}_{i-1}, \bar{z}_i, x_{i+1} \dots x_n$  vermöge (35) Nullstelle von  $\mathfrak{b}$ . Bedeutet also  $H^{(i)}(z, x)$  den größten gemeinsamen Teiler aller Polynome aus  $\mathfrak{b}_i$ , der als ganz und primitiv in den  $v$  vorausgesetzt werden darf — so erhält  $H^{(i)}(z, x)$  nach dem letzten Teil von Satz XII den Faktor  $z_i - \bar{z}_i = z_i - (\bar{x}_i + v_1 \bar{x}_1 + \dots + v_{i-1} \bar{x}_{i-1})$ , und jeder Nullstelle von  $\alpha$ , die bei Adjunktion von  $x_{i+1}, \dots, x_n$  auftritt, entspricht ein solcher Faktor. Es ist zu zeigen, daß damit die Zerlegung von  $H^{(i)}(z, x)$  erschöpft ist; d. h. daß sich aus  $H^{(i)}$  kein Faktor  $H_1^{(i)}$  abspalten läßt, der sich nicht in Linearfaktoren in  $z_i$  und  $v$  zerlegen läßt. Sei dies der Fall, so enthält  $H_1^{(i)}$  wegen der vorausgesetzten Primitivität in  $v$  mindestens einen Linearfaktor  $z_i - \bar{z}_i$ , wo  $\bar{z}_i$  einem algebraischen Erweiterungskörper von  $P(u, v, x_{i+1} \dots x_n)$  angehört. Ist  $\bar{x}_1 \dots \bar{x}_{i-1}, \bar{z}_i, x_{i+1} \dots x_n$  die entsprechende Nullstelle von  $\alpha$ , so muß diese mit einer der endlich vielen Nullstellen von  $\alpha$  zusammenfallen, die bei Adjunktion von  $x_{i+1} \dots x_n$  auftreten, also von  $v$  unabhängig sein. Somit enthält  $\bar{z}_i$  die  $v$  notwendig linear, nicht algebraisch oder rational-nichtlinear; aus  $H_1^{(i)}$  läßt sich gegen



die Annahme ein weiterer Linearfaktor  $z_i - (\bar{x}_i + v_1 \bar{x}_1 + \dots + v_{i-1} \bar{x}_{i-1})$  in  $z$  und  $v$  abspalten. Somit kommt als explizite Zerlegung:

$$H^{(i)}(z, x) = \prod \{z_i - (\bar{x}_i + v_1 \bar{x}_1 + \dots + v_{i-1} \bar{x}_{i-1})\}^{\alpha_i}.$$

Da der Grad von  $H^{(i)}$  und die einzelnen Exponenten  $\alpha_i$  mit den entsprechenden von  $D^{(i)}(x)$  übereinstimmen müssen — denn  $H^{(i)}$  entsteht aus  $D^{(i)}$  durch die Spezialisierung  $u_{\mu\nu} = v_{\mu\nu}$ ,  $D^{(i)}$  aus  $H^{(i)}$  durch die Spezialisierung  $v = 0$  —, so zeigt diese Zerlegung noch, daß wegen der Adjunktion der Unbestimmten  $u_{\mu\nu}$  zu  $P$  auch bei der von  $\alpha$  ausgehenden Elimination jeder Nullstelle  $\bar{x}_i$  von  $D^{(i)}$  ein jeweils *linearer* größter gemeinsamer Teiler aus  $\alpha_{i-1} \dots \alpha_1$  oder die Potenz eines solchen entspricht, sich also jeweils nur *ein* zusammengehöriges Nullstellensystem  $\bar{x}_1 \dots \bar{x}_i, x_{i+1} \dots x_n$  von  $\alpha$  ergibt<sup>18)</sup>.

## § 7.

### Resultantenform und Eliminationstheorie.

Zur Herstellung des Zusammenhanges zwischen Resultantenform und Eliminationstheorie werde die in § 6 gegebene sukzessive Elimination speziell auf den *Quotienten*  $\alpha = m/g_{i-1}$  von Ideal durch Grundideal  $i-1$ -ter Stufe angewandt. Es ist zuerst zu zeigen, daß dieser Quotient ein transformiertes Ideal darstellt. Nun ist  $m$  transformiert und folglich nach Satz VI, § 3, auch  $g_{i-1}$ . Aus

$$H(x) \equiv 0 \pmod{m/g_{i-1}}; \quad H(x) = \bar{H}(y) = \sum \alpha_i(u) \bar{H}_i(y) = \sum \alpha_i(u) H_i(x)$$

folgt also:

$$\bar{H}(y) \cdot \bar{g}_{i-1} \equiv 0 \pmod{\bar{m}_{(u)}}; \quad \text{also auch} \quad \bar{H}(y) \bar{g}_{i-1} \equiv 0 \pmod{\bar{m}_{(u)}}$$

oder

$$\bar{H}_i(y) \bar{g}_{i-1} \equiv 0 \pmod{\bar{m}}, \quad \text{also} \quad H_i(x) g_{i-1} \equiv 0 \pmod{m},$$

womit die Teilbarkeit von  $H_i(x)$  durch  $m/g_{i-1}$  und damit dieses Ideal als transformiert nachgewiesen ist, so daß die Eliminationsmethode des § 6 anwendbar wird.

Nun zeigt aber (30), unter Berücksichtigung von (28) — § 4 —, daß  $C^{(i)}(x)$  durch  $m/g_{i-1}$  teilbar ist, unter  $C^{(i)}(x)$  irgendeine nicht identisch verschwindende Determinante  $\varrho$ -ten Grades aus  $\mathfrak{M}_{i-1}^*$  verstanden. Da  $C^{(i)}$

<sup>18)</sup> Es sei darauf hingewiesen, daß die hier gegebene sukzessive Elimination — im Gegensatz zu der Kroneckerschen Methode — nur von dem gegebenen Ideal  $\alpha$  abhängt, unabhängig von jeder Idealbasis ist, was also insbesondere auch für die Exponenten  $\alpha_i$  gilt. Die vollständige Durchführung der Elimination nach dieser Methode würde nach Hentzelt die Fortsetzung des Verfahrens auf den Quotienten  $\alpha_i/D^{(i)}$  verlangen, was mit Rücksicht auf den nächsten Paragraphen unterbleiben mag. (E. N.)

für  $i > 1$  nullten Grades in  $x_1$  ist, enthält also der dem Ideal  $\alpha = \alpha_i$  entsprechende Modul  $\mathfrak{A}_i$  die Polynome  $C^{(i)}, x_1 C^{(i)}, \dots, x_1^{k_1-1} C^{(i)}$ , und folglich ist  $(C^{(i)})^{k_1}$  durch  $\alpha_i$  teilbar; ebenso wird  $(C^{(i)})^{k_1 k_2}$  durch  $\alpha_3$  teilbar, und schließlich  $(C^{(i)})^{k_1 k_2 \dots k_{i-1}}$  teilbar durch  $\alpha_i$ . Somit werden  $\alpha_1, \dots, \alpha_i$  vom Nullideal verschieden, was auch für  $i=1$  gilt. Sei jetzt  $D^{(i)}(x)$  der größte gemeinsame Teiler aller Polynome aus  $\alpha_i$ , also nur dann von einem Grade  $p_i > 0$ , wenn  $\alpha_{i+1}$  gleich dem Nullideal wird. Nach der Definition von  $D^{(i)}(x)$  kommt unter Berücksichtigung der Teilbarkeit von  $\alpha_i$  durch  $\alpha$ :

$$d^{(i+1)} D^{(i)}(x) \equiv 0 \pmod{g_{i-1}} \quad d^{(i+1)} \neq 0;$$

es wird also  $d^{(i+1)} D^{(i)}$  ein von  $x_1 \dots x_{i-1}$  freies Polynom aus  $m/g_{i-1}$ . Nun war aber  $E^{(i)}(x)$  als höchster Elementarteiler von  $\mathfrak{M}_{i-1}$  bzw.  $\mathfrak{M}_{i-1}^*$  definiert (Satz II und § 4) als größter gemeinsamer Teiler — im Polynom-sinn — aller von  $x_1 \dots x_{i-1}$  freien Polynome aus  $m/g_{i-1}$ . Somit wird  $d^{(i+1)} D^{(i)}$ , und wegen der Regularität von  $E^{(i)}(x)$  in  $x_i$ , auch  $D^{(i)}(x)$  durch  $E^{(i)}(x)$  teilbar. (Klein, 19, 1, 1)

Dieselbe Überlegung läßt sich durchführen, wenn von vornherein die Transformation (12) mit (35) zusammengesetzt war, d. h. wenn die Unbestimmten  $u_{\mu\nu}$  durch  $w_{\mu\nu}$  ersetzt waren, was die Teilbarkeit von  $H^{(i)}(z, x)$  durch das entsprechende  $\bar{E}^{(i)}(z, x)$  ergibt. Da ebenso wie  $D^{(i)}(x)$  und  $H^{(i)}(z, x)$  auch  $E^{(i)}(x)$  und  $\bar{E}^{(i)}(z, x)$  und ebenso  $R^{(i)}(x)$  und  $R^{(i)}(z, x)$  gegenseitig durch Spezialisierung auseinander hervorgehen, so müssen auch hier die Vielfachheitszahlen bei der Zerlegung in Linearfaktoren gegenseitig übereinstimmen. Berücksichtigt man noch, daß eine Potenz von  $E^{(i)}(x)$  durch  $R^{(i)}(x)$  teilbar ist, so kommt zusammenfassend:

**Satz XIII.** *Zerlegt man  $R^{(i)}(x)$  in einem algebraischen Erweiterungskörper von  $P(u, x_{i+1} \dots x_n)$  in Linearfaktoren  $x_i - \bar{x}_i$ , so läßt sich  $\bar{x}_i$  auf eine und nur eine Art zu einem zusammengehörigen Wertsystem  $\bar{x}_1 \dots \bar{x}_i, x_{i+1} \dots x_n$  ergänzen, das Nullstelle von  $m/g_{i-1}$  und folglich von  $m$  wird. Die derart aus den Linearfaktoren von  $R^{(i)}$  entspringenden, endlich vielen Nullstellen von  $m$  — endlich viele nach Adjunktion von  $x_{i+1} \dots x_n$  — werden zusammengefaßt durch die explizite Zerlegung:*

$$(36) \quad \bar{R}^{(i)}(z, x) = \prod \{z_i - (\bar{x}_i + v_1 \bar{x}_1 + \dots + v_{i-1} \bar{x}_{i-1})\}^{l_i}.$$

Diese Zerlegung bleibt wegen der Regularität von  $\bar{R}^{(i)}(z, x)$  in  $z_i$  erhalten, wenn die zu  $P(u)$  adjungierten  $x_{i+1} \dots x_n$  durch irgendwelche speziellen Wertsysteme  $\bar{x}_{i+1} \dots \bar{x}_n$  aus  $P(u)$  oder dem daraus abgeleiteten algebraisch-abgeschlossenen Körper ersetzt werden.

Damit ist zugleich eine Trennung der Nullstellen von  $m$  nach den einzelnen Faktoren der Resultantenform durchgeführt; die Anzahl der zu

$P(u)$  adjungierten Unbestimmten  $x$  wird auch als *Dimension* des entsprechenden algebraischen Gebildes bezeichnet.

Faßt man in der Zerlegung von  $R^{(i)}(z, x)$  oder der entsprechenden von  $R^{(i)}(x)$  die in bezug auf  $P(u, x_{i+1} \dots x_n)$  konjugierten Faktoren zusammen, die bei allgemeinem  $P$  ganz oder teilweise identisch sein können, so kommt eine Zerlegung von  $R^{(i)}(x)$  in Potenzen von in bezug auf  $P(u, x_{i+1} \dots x_n)$  irreduziblen Polynomen:

$$R^{(i)}(x) = S_1^{(i)}(x)^{\beta_1} \dots S_n^{(i)}(x)^{\beta_n}.$$

Dieser Zerlegung entspricht nach Satz X eine Darstellung  $g_i = [j_1 \dots j_n]$ , derart, daß  $S_\mu^{(i)}(x)^{\beta_\mu}$  gleich der Norm von  $g_{i-1}$  nach dem Ideal  $j_\mu$  wird, bzw. gleich der Norm des Moduls  $\mathfrak{G}_{i-1}$  nach dem  $j_\mu$  entsprechenden Modul. Damit ist also auch die *Bedeutung der Exponenten*  $\beta_\mu$  klargelegt; insbesondere wird — unter  $\gamma_\mu$  den Grad von  $S_\mu^{(i)}$  verstanden — die Multiplizität  $\beta_\mu \gamma_\mu$  gleich der *Anzahl der in bezug auf*  $P(u, x_{i+1} \dots x_n)$  *linear unabhängigen Restklassen von*  $g_{i-1}$  *nach*  $j_\mu$ .

Es sei noch kurz der spezielle Fall betrachtet, wo  $P$  von der Charakteristik Null ist. Spezialisiert man hier die  $u_\mu$ , so zu Größen  $\bar{u}_\mu$ , aus  $P$ , daß die  $n$  Determinanten  $O^{(i)}(x)$  ( $i = 1, 2, \dots, n$ ) jeweils in  $x_i$  regulär bleiben<sup>19)</sup>, so bleibt auch die Regularität von  $R^{(i)}$  erhalten. Es wird  $R^{(i)}$  und ebenso  $R^{(i)}(z, x)$  bei dieser Spezialisierung ein gemeinsamer Teiler aller  $\varrho$ -reihigen Determinanten aus  $\mathfrak{M}_{i-1}^*$ , aber nicht notwendig der größte gemeinsame Teiler. Man kann aber die Spezialisierung immer so vornehmen, daß auch diese letztere Eigenschaft erhalten bleibt. Denn  $\bar{R}^{(i)}(z, x)$  läßt sich — wie die Existenz der Modulbasis zeigt — auch charakterisieren als größter gemeinsamer Teiler von endlich vielen  $\varrho$ -reihigen Determinanten aus  $\mathfrak{M}_{i-1}^*$ . Die Zerlegung des so spezialisierten  $\bar{R}^{(i)}(z, x)$  ergibt sich dann einfach durch Ersetzen der  $u_\mu$  durch  $\bar{u}_\mu$  in (36), so daß die ganze Eliminationstheorie erhalten bleibt.

<sup>19)</sup> Hentzelt nimmt von vornherein diese Spezialisierung für die  $u_\mu$  vor und muß deshalb auch zum Nachweis der Zerlegbarkeit von  $H^{(i)}(z, x)$ , bzw.  $\bar{R}^{(i)}(z, x)$  in Linearfaktoren in  $z$  und  $v$  viel kompliziertere Betrachtungen zu Hilfe nehmen. Die dabei auftretenden Exponenten brauchen nicht notwendig mit den obigen übereinzustimmen. (E. N.)