Werk

Titel: Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. (Unter Be...

Autor: Hermann, G.

Jahr: 1926

PURL: https://resolver.sub.uni-goettingen.de/purl?235181684_0095|log44

Die Frage der endlich vielen Schritte in der Theorie der Polynomideale.

(Unter Benutzung nachgelassener Sätze von K. Hentzelt.)

Von

Grete Hermann in Göttingen.

Die Ringbereiche, in denen die in der vorliegenden Arbeit auftretenden Ideale definiert sind, sollen Polynombereiche sein. Ein Ideal soll *gegeben* heißen, wenn eine *Basis* des Ideals bekannt ist, es heißt *berechenbar*, wenn sich eine *Basis* berechnen läßt. In dieser Arbeit soll es sich darum handeln, die für ein gegebenes Ideal $\mathfrak{m}$ charakteristischen Ideale und Polynome zu berechnen. Die Berechnung stützt sich dabei auf die Ideal- und Eliminationstheorie, wie sie von E. Noether und K. Hentzelt entwickelt ist [1]). Für die benutzten Grundbegriffe verweise ich insbesondere auf die Zusammenstellung N. § 1. Einige Änderungen in den Definitionen und weitere Zusätze werden in § 1 dieser Arbeit gegeben.

Die folgenden Rechenmethoden werden Berechnungen mit *endlich vielen Schritten* sein. Die Behauptung, eine Berechnung kann mit endlich vielen Schritten durchgeführt werden, soll dabei bedeuten, es kann eine *obere Schranke für die Anzahl der zur Berechnung notwendigen Operationen* angegeben werden. Es genügt also z. B. nicht, ein Verfahren anzugeben, von dem man theoretisch nachweisen kann, daß es mit endlich vielen Operationen zum Ziele führt, wenn für die Anzahl dieser Operationen keine obere Schranke bekannt ist [2]). Die in der vorliegenden Arbeit

[1]) E. Noether, Idealtheorie in Ringbereichen, Math. Annalen **83** (1921), S. 24–66. K. Hentzelt, Zur Theorie der Polynomideale u. Resultanten, bearbeitet von E. Noether, Math. Annalen **88** (1922), S. 53–79, zitiert H. N. E. Noether, Eliminationstheorie und allgemeine Idealtheorie, Math. Annalen **90** (1923), S. 229–261, zitiert N. Für die benutzten Begriffe der Körpertheorie sei verwiesen auf E. Steinitz, Algebraische Theorie der Körper, Journal für Mathematik **137** (1910), S. 167–309, zitiert St.

[2]) Macaulay, der im Anschluß an die Laskersche Arbeit [Zur Theorie der Moduln und Ideale, Math. Annalen **60**] Wege zur Berechnung der zu einem Ideal

auftretenden Schranken werden dabei speziell nur von der Anzahl n der Variablen, der Anzahl t der Basiselemente des Ideals und dem Maximalgrad q dieser Basiselemente abhängen, sie sind unabhängig von den Koeffizienten dieser Basiselemente. Mit Hilfe dieser Schranken, die angeben, bis zu welchem Grad die Variablen berücksichtigt werden müssen, werden sich die Probleme zurückführen lassen auf Probleme der Determinanten- und Elementarteilertheorie, die sich nach bekannten Methoden mit endlich vielen Schritten erledigen lassen.

Den in §§ 6—8 gelieferten Methoden, mit denen sich alle für das Ideal $\mathfrak{m}$ charakteristischen Ideale und Polynome berechnen lassen, müssen in §§ 2—5 einige vorbereitende Sätze vorausgeschickt werden. Das Aufsuchen der zu einem Ideal $\mathfrak{m}$ gehörigen Primideale entspricht dem einfacheren Problem der Zerlegung eines Polynoms in Primfunktionen und führt auch darauf zurück. § 2 wird deshalb zunächst die Zerlegung eines Polynoms in Primfunktionen behandeln. Die hier benutzten Methoden sind von Kronecker[3]) angegeben. Kronecker beschränkt sich allerdings auf Körper der Charakteristik Null, und in ihnen nur auf endliche algebraische und transzendente Erweiterung des Primkörpers. Seine Methoden lassen sich direkt auf Körper beliebiger Charakteristik, und zwar auf endliche algebraische und endliche oder unendliche transzendente Erweiterungen des Primkörpers ausdehnen. Für den Fall unendlicher algebraischer Erweiterungen muß man Steinitzsche Überlegungen zu Hilfe nehmen.

Die Sätze der weiteren Paragraphen sind idealtheoretisch. In §§ 3—5 werden die Grundlagen zur Berechnung der oberen Schranken gegeben, die die späteren Berechnungen erst ermöglichen. Zunächst ist es notwendig, daß die einfachsten Rechenoperationen der Idealtheorie, die Bildung von Produkt und Quotient, kleinstem gemeinsamen Vielfachen und größtem gemeinsamen Teiler mit endlich vielen Schritten durchgeführt werden können. Die Methoden dafür werden sich, soweit sie nicht trivial sind, in § 3 als Anwendungen eines Hilbertschen Satzes[4]) ergeben. §§ 4 und 5 bringen Kriterien für die Teilbarkeit eines Polynoms durch ein Ideal, und

---

gehörigen Primideale und der Exponenten von Primäridealen angibt, hat keine solche obere Schranke. Macaulay, On the Resolution of a given Modular System, Math. Annalen 74, Anmerkung *), S. 81.

[3]) Kronecker, Grundzüge einer arithmetischen Theorie der algebraischen Größen, § 4, Journal für Math. 92 (1882), S. 1—122.

[4]) Hilbert, Über die Theorie der algebraischen Formen, Math. Annalen 36 (1890), S. 473—534. Der hier benutzte Satz ist ein Teil des Theorems 3 über das Abbrechen der Syzygienkette. Derselbe Satz steht auch bei König [J. König, Einleitung in die allgemeine Theorie der algebraischen Größen]. König benutzt dieselbe Methode wie Hilbert, geht aber fälschlich von nur einer Gleichung aus, ohne zu bemerken, daß der Induktionsschluß doch auf ein Gleichungssystem führt.

zwar ist das in § 4 gelieferte Kriterium rein formal, die Teilbarkeit hängt von der Lösbarkeit eines linearen Gleichungssystems ab, das sich aus den Koeffizienten des gegebenen Polynoms und denen der Basiselemente des Ideals berechnen läßt. Es ist zur Anwendung dieses Kriteriums also nicht nötig, daß man den inneren Aufbau des Ideals kennt. Dagegen liefert der in § 5 gebrachte *Hentzeltsche Nullstellensatz* ein Kriterium, das zugleich inhaltlich Aufschluß über den Bau des Ideals gibt. Er gibt nämlich eine Schranke für den Grad, in dem ein Polynom mindestens in den transzendenten Nullstellen des Ideals verschwinden muß, um durch das Ideal teilbar zu sein. Wegen seiner begrifflichen Fassung ist dieses Kriterium gegenüber dem in § 4 gegebenen schon an sich von eigenem Interesse; im speziellsten Fall kommt es auf den Noetherschen Fundamentalsatz der algebraischen Funktionen zurück. Außerdem aber wird sich zeigen, daß die hier berechnete Zahl bereits eine obere Schranke ist für den kleinsten Exponenten von Primäridealen, die in einer Zerlegung von $\mathfrak{m}$ auftreten können.

Als Anwendungen der Sätze von §§ 2—5 ergeben sich nun in §§ 6—8 die Berechnungen der wesentlichen Ideale und Polynome. § 6 liefert zunächst die Berechnung der Grundideale, bei der sich gleichzeitig die Berechnung von Norm und Elementarteilerform des Ideals ergibt. Damit sind die für die Eliminationstheorie wesentlichen Polynome berechnet, aus deren Zerlegung man die Nullstellen des Ideals erhält. In § 7 werden Methoden zur Berechnung der zum Ideal $\mathfrak{m}$ gehörigen Primideale angegeben; diese werden komplizierter, wenn der für die Polynome des Ideals zugrunde gelegte Koeffizientenbereich ein unvollkommener Körper ist, als im Fall des vollkommenen Körpers. In § 8 wird schließlich gezeigt, wie man unter Anwendung des Hentzeltschen Nullstellensatzes zu jedem zum Ideal $\mathfrak{m}$ gehörigen Primideal ein Primärideal findet, das in einer Zerlegung von $\mathfrak{m}$ auftreten kann. Mit diesen Primäridealen hat man natürlich auch die isolierten Komponenten des Ideals.

Die Sätze von §§ 4 und 5, sowie Satz 6 in § 6 sind einem Manuskript von K. Hentzelt entnommen. Hentzelt gibt sie dort allerdings nur in recht unübersichtlichen Formeln, denen die begriffliche Deutung fehlt. Ich habe diese Fassung durch eine begriffliche ersetzt und die Schranken, deren Berechnung Hentzelt nur andeutet, explizit angegeben. Ferner war es beim Hentzeltschen Nullstellensatz nötig, die Behauptung durch Benutzung des Begriffs der transzendenten Nullstelle etwas zu erweitern. Hentzelt spricht nur von der Gesamtheit der algebraischen Nullstellen eines Ideals und hat so nicht die für das Folgende wesentliche Einteilung der Nullstellen nach der Dimension der Primideale. Die in den Hentzeltschen Beweisen benutzte Methode des Reduzierens der Gradzahlen durch

eine reguläre Determinante — d. h. durch eine Determinante, die ein reguläres Polynom darstellt — hat Hentzelt aus dem Hilbertschen Beweis, der in § 3 gebracht ist, übernommen, so daß die Beweise der Sätze in §§ 3—5 ganz parallel laufen. Hentzelt bezweckte mit seinen Sätzen nur die Erledigung der Fragen der Eliminationstheorie mit endlich vielen Schritten, er wollte Norm und Elementarteilerform eines Ideals berechnen. Wie die Anwendungen §§ 6—8 zeigen, lassen sich aber bereits alle für das Ideal charakteristischen Ideale unter Zugrundelegung seiner Sätze berechnen.

§ 1.

Grundbegriffe.

Die Definitionen des zugrunde gelegten Bereichs, des transformierten Ideals, der Moduldarstellung des Ideals, seiner isolierten Komponenten, der Elementarteilerform und Norm, sowie die für Ideale gültigen Zerlegungssätze sind gegeben N. § 1, 1—3, 5—7, 9.

1. *Bezeichnungen.* Es bezeichne $[f]$ den Grad des Polynoms $f(x_1 \dots x_n)$ in allen Variablen; $[f]_\varrho$ den Grad von f in $x_1 \dots x_\varrho$. $f^{(i)}$, $g^{(i)}$, $h^{(i)}$ usw. sollen nur von $x_i \dots x_n$ abhängende Polynome bedeuten.

Bezeichnet P irgendeinen Körper, und sind $\alpha_1 \dots \alpha_\nu$ irgendwelche in einem Erweiterungskörper von P gelegene, in bezug auf P algebraische oder transzendente Größen, so bedeute $\mathsf{P}(\alpha_1 \dots \alpha_\nu)$ den aus P durch Adjunktion der $\alpha_1 \dots \alpha_\nu$ hervorgehenden Körper, $\mathsf{P}[\alpha_1 \dots \alpha_\nu]$ den Ring der Polynome in $\alpha_1 \dots \alpha_\nu$ mit Koeffizienten aus P. Ist $\overline{\mathsf{P}}$ der den nicht transformierten Idealen zugrunde liegende Körper, P der der transformierten, so ist mit diesen Bezeichnungen nach N. § 1, 1

$$\mathsf{P} = \overline{\mathsf{P}}(u_{11} \dots u_{nn}),$$

wo die u_{ij} die Transformationskoeffizienten bedeuten, während sich die Ringbereiche $\overline{\mathfrak{R}}$ und $\mathfrak{R}$ der nicht transformierten und der transformierten Ideale so schreiben lassen:

$$\overline{\mathfrak{R}} = \overline{\mathsf{P}}[y_1 \dots y_n],$$
$$\mathfrak{R} = \mathsf{P}[x_1 \dots x_n] = \overline{\mathsf{P}}(u_{11} \dots u_{nn})[x_1 \dots x_n].$$

2. *Die Dimension* eines vom Einheitsideal $\mathfrak{o}$ verschiedenen Primideals sei nun im Gegensatz zu N. § 1, 8 auf folgende Weise definiert: Der Restklassenring von $\overline{\mathfrak{R}}$ nach einem von $\mathfrak{o}$ verschiedenen Primideal $\overline{\mathfrak{p}}$ ist nach Definition ein Ring ohne Nullteiler, kann also zu einem Restklassenkörper $\overline{\mathfrak{R}} \,|\, \overline{\mathfrak{p}}$ durch Adjunktion von Elementenpaaren erweitert werden. $\overline{\mathfrak{R}} \,|\, \overline{\mathfrak{p}}$ ist Erweiterungskörper von einem zu $\overline{\mathsf{P}}$ isomorphen Körper $(\overline{\mathsf{P}})$. Der Transzendenzgrad ν von $\overline{\mathfrak{R}} \,|\, \overline{\mathfrak{p}}$ in bezug auf $(\overline{\mathsf{P}})$ heißt Transzendenz-

grad oder Dimension von $\bar{\mathfrak{p}}$, und es wird $0 \leqq \nu \leqq n$. Daß diese Definition sachlich mit der von N. § 1, 8 übereinstimmt, folgt direkt aus N. Satz 5.

3. Die Definition der *Grundideale* soll sich nun sachgemäß an die der Dimension der Primideale anschließen. Die isolierte Komponente des Ideals $\mathfrak{m}$, zu der alle zu $\mathfrak{m}$ gehörigen Primideale $n - \varrho$-ter und höherer Dimension und nur diese gehören, heißt das ϱ-te Grundideal $\mathfrak{g}_\varrho$ von $\mathfrak{m}$. Es folgt sofort: $\mathfrak{g}_{\varrho-1}$ ist das $\varrho - 1$-te Grundideal von $\mathfrak{g}_\varrho$; $\mathfrak{g}_\varrho$ ist mit seinem ϱ-ten Grundideal identisch. Ideale, für die das erste von $\mathfrak{o}$ verschiedene Grundideal mit dem Ideal identisch ist, haben nur zugehörige Primideale einer bestimmten Dimension. Nach N. Satz 8 und 10 stimmt auch diese Definition für transformierte Ideale mit der N. § 1, 4 gegebenen überein, so daß auch darauf zurückgegriffen werden kann.

4. Neben transformierten Idealen werden auch *transformierte Moduln und Gleichungssysteme* auftreten. Ein Modul aus Linearformen mit Koeffizienten aus $\mathsf{P}[x_1 \ldots x_n]$ heißt transformiert, wenn er durch die Transformation $y = U(x)$ und die Adjunktion der unbestimmten Transformationskoeffizienten zum Körper $\overline{\mathsf{P}}$ aus einem Linearformenmodul mit Koeffizienten aus $\overline{\mathsf{P}}[y_1 \ldots y_n]$ hervorgegangen ist. Ebenso heißt ein lineares Gleichungssystem mit Koeffizienten aus $\mathsf{P}[x_1 \ldots x_n]$ transformiert, wenn es durch $y = U(x)$ aus einem linearen Gleichungssystem mit Koeffizienten aus $\overline{\mathsf{P}}[y_1 \ldots y_n]$ hervorgegangen ist. Bei transformierten Moduln und Gleichungssystemen kann stets die Existenz einer nicht verschwindenden Determinante, deren Rang mit dem von Modul oder Gleichungssystem übereinstimmt, vorausgesetzt werden, die ein in bezug auf x_i $[i = 1 \ldots n]$ reguläres Polynom darstellt. Eine solche Determinante soll auch als reguläre Determinante bezeichnet werden.

Nach N. Hilfssatz 1 gehen Prim- und Primärideale durch die Transformation $y = U(x)$ wieder in Prim- und Primärideale über. Es gilt auch das Umgekehrte. Transformierten Prim- und Primäridealen entsprechen bei den nicht transformierten Idealen wieder Prim- und Primärideale. Es sei nämlich $\mathfrak{q}$ ein transformiertes Primärideal, $\bar{\mathfrak{q}}$ das entsprechende nicht transformierte Ideal. $\bar{a}$ und $\bar{b}$ seien Größen aus $\overline{\mathfrak{R}}$, a und b die durch Transformation daraus hervorgehenden Polynome. Dann folgt aus $\bar{a} \cdot \bar{b} \equiv 0\,(\bar{\mathfrak{q}})$, $\bar{b}^\varkappa \not\equiv 0\,(\bar{\mathfrak{q}})$ für jedes $\varkappa$, auch $a \cdot b \equiv 0\,(\mathfrak{q})$, $b^\varkappa \not\equiv 0\,(\mathfrak{q})$ für jedes $\varkappa$, es wird also $a \equiv 0\,(\mathfrak{q})$ und folglich auch $\bar{a} \equiv 0\,(\bar{\mathfrak{q}})$. $\bar{\mathfrak{q}}$ ist also Primärideal. Ist $\mathfrak{q}$ Primideal, und ersetzt man dementsprechend in diesen Überlegungen $\varkappa$ durch 1, so ergibt sich: $\bar{\mathfrak{q}}$ ist Primideal. Da Teilbarkeiten beim Hin- und Hertransformieren erhalten bleiben, so gehen zugehörige Prim- und Primärideale in zugehörige über. Ferner wird die Dimension eines Primideals durch die Transformation nicht geändert [vgl. N. Fußnote [12])]. Nach N. Hilfs-

satz 2 kann man in der Darstellung eines nicht transformierten Ideals als kleinstes gemeinsames Vielfaches größter primärer Ideale die ursprünglichen Komponenten einzeln transformieren, und erhält so eine Darstellung des transformierten Ideals als kleinstes gemeinschaftliches Vielfaches größter primärer Komponenten. Da die Dimension dieser Komponenten erhalten bleibt, so ist also nach der Definition des Grundideals das ϱ-te Grundideal des transformierten Ideals das transformierte Ideal des ϱ-ten Grundideals des nicht transformierten Ideals, denn die entsprechenden Primideale gehen ineinander über, und ebenso gehen die isolierten Komponenten des nicht transformierten Ideals durch Transformation in die des transformierten Ideals über.

Da sich nun der Übergang vom transformierten zum nichttransformierten Ideal mit endlich vielen Schritten ausführen läßt — Rückgängigmachen der Transformation, Aufspalten der Basiselemente nach Potenzprodukten der Transformationskoeffizienten —, so kann man sich bei der Berechnung der Basiselemente der zu einem Ideal $\mathfrak{m}$ gehörenden Prim-, Primär- und Grundideale und der isolierten Komponenten auf transformierte Ideale beschränken. Sofern diese Ideale nämlich eindeutig sind, sind sie mit $\mathfrak{m}$ auch transformiert. Die Primärideale sind die einzigen nicht eindeutigen. Bei ihrer Berechnung wird also extra nachzuweisen sein, daß man transformierte Ideale bekommt.

5. *Die Elementarteilerform eines Primideals im vollkommenen und unvollkommenen Körper.* Der Körper P heißt vollkommen, wenn jede Primfunktion in ihm in einem geeigneten Erweiterungskörper in getrennte Linearfaktoren zerfällt, im entgegengesetzten Fall heißt P unvollkommen. Es gilt der Satz: Die Elementarteilerform eines Primideals ist eine Primfunktion, die eines Primärideals ist eine Potenz der Primfunktion, welche Elementarteilerform des zugehörigen Primideals ist [N. Satz 1]. Im vollkommenen Körper gilt die Umkehrung: Ist die Elementarteilerform eines Ideals Primfunktion, so ist das Ideal Primideal [N. Satz 13]. Im unvollkommenen Körper gilt nur: Ist die Elementarteilerform eines Ideals [echte oder unechte] Primärfunktion, so ist das Ideal [echtes oder unechtes] Primärideal; es kann im unvollkommenen Körper echte Primärideale geben, deren Elementarteilerform Primfunktion ist [N. § 6, Beispiel 2].

§ 2.

Polynomzerlegung in endlich vielen Schritten.

Vorgelegt sei ein Polynom $f(x_1 \dots x_n)$ in einem Körper P; es wird gefragt nach der Zerlegung von f in Primfaktoren in einem Erweiterungs-

körper von P, und zwar nach einer Zerlegung mit endlich vielen Schritten. Durch die Kroneckersche Substitution

$$x_\lambda = \xi^{d^{(n-\lambda)}},$$ [5])

in der d größer gewählt werden muß als der Grad von f, kann dem f eindeutig ein Polynom mit nur einer Variablen ξ zugeordnet werden, derart, daß jedem Teiler von f ein Teiler dieses Polynoms entspricht. Wegen der eindeutigen Zuordnung der Polynome ist deshalb mit der Gesamtheit der Teiler des Polynoms in ξ auch die Gesamtheit der Teiler von f bekannt. Man kann sich also auf die Zerlegung von Polynomen einer Variablen beschränken. Es wird sich zeigen, daß die Möglichkeit der Zerlegung abhängt von der Beschaffenheit des Körpers, in dem zerlegt werden soll. Am einfachsten ist das Problem, wenn der Erweiterungskörper aus dem Primkörper durch Adjunktion endlich vieler algebraischer und transzendenter Elemente hervorgeht. Hier gilt der Kroneckersche Satz [6]).

Satz 1. Voraussetzung. *K sei Primkörper, $z_k\,[k = 1 \dots m]$ sei transzendent in bezug auf $K(z_1 \dots z_{k-1}; z_{k+1} \dots z_m; \alpha_1 \dots \alpha_l)$; $\alpha_i\ [i = 1 \dots l]$ sei algebraisch in bezug auf $K(z_1 \dots z_m; \alpha_1 \dots \alpha_{i-1}; \alpha_{i+1} \dots \alpha_l)$.*

Behauptung: *In $\mathsf{P} = K(z_1 \dots z_m \alpha_1 \dots \alpha_l)$ läßt sich jedes Polynom $f(x)$ mit endlich vielen Schritten in Primfaktoren zerlegen.*

Beweis durch zweimaliges Anwenden der vollständigen Induktion.

1. $l = 0$. Der Fall $m = 0$ muß verschieden behandelt werden, je nachdem die Charakteristik von K den Wert 0 hat oder eine Primzahl p ist. Im zweiten Fall ist der Beweis sehr einfach, da dann $\mathsf{P} = K$ nur endlich viele Elemente enthält; im ersten Fall läuft der Beweis dem Schluß von $n - 1$ auf n ganz parallel, so daß er mit diesem zusammen gebracht werden kann.

a) Es sei also zunächst $m = l = 0$; $\mathsf{P} = K$ sei von der Charakteristik p, habe also nur p Elemente. Ist nun $f(x)$ vom Grade r, so brauchen als Teiler nur Polynome vom Grade $q \leqq \frac{r}{2}$ untersucht zu werden. Da K nur p Elemente hat, die als Koeffizienten dieser Polynome in Frage kommen, so gibt es nur $p^{\left(\left[\frac{r}{2}\right]+1\right)}$ Polynome von einem Grad $q \leqq \frac{r}{2}$. Dabei bedeutet

[5]) J. König, Einleitung in die allgemeine Theorie der algebraischen Größen. Leipzig 1903, Kapitel II, §§ 3 und 4.

[6]) Siehe Fußnote [3]), Kronecker beweist den Satz allerdings nur für den Fall der Charakteristik 0, wo endlich viele algebraische Erweiterungen in eine einzige zusammengefaßt werden können. Die dabei benutzten Methoden lassen sich aber sofort auf den allgemeineren Fall übertragen.

$\left[\frac{r}{2}\right]$ die größte ganze Zahl $\leqq \frac{r}{2}$. Diese Polynome können einzeln mit endlich vielen Schriften daraufhin geprüft werden, ob sie Teiler von f sind oder nicht.

b) P enthalte unendlich viele Elemente, sei also entweder der Primkörper K von der Charakteristik 0, oder $\mathsf{P} = K(z_1 \ldots z_m)$. Es bedeute $[K]$ den in K gelegenen Ring, der dem Ring aller ganzen Zahlen isomorph ist, falls K von der Charakteristik 0 ist; andernfalls sei $[K] = K$. Es sei $[\mathsf{P}] = [K][z_1 \ldots z_m]$. Ohne Beschränkung der Allgemeinheit kann $f(x)$ als Größe aus $[\mathsf{P}][x]$ angenommen werden; ferner braucht man nach bekannten Sätzen über primitive Funktionen nur die Teiler von f zu berücksichtigen, die ebenfalls in $[\mathsf{P}][x]$ liegen.

Es sei $q \leqq \frac{r}{2}$. Wir fragen nach der Existenz eines Teilers $\varphi(x)$ vom Grade q. Es seien $s_0 \ldots s_q$ irgendwelche $q+1$ verschiedene Elemente aus $[K][z_1]$. Ist K von der Charakteristik 0, so enthält K bereits unendlich viele Zahlen, in diesem Fall sollen die $s_0 \ldots s_q$ bereits Größen aus $[K]$ sein. Dann wird:

$$\varphi(x) = \varphi(s_0) g_0(x) + \ldots + \varphi(s_q) g_q(x).$$

Dabei ist:

$$g_i(x) = \frac{(x-s_0)\ldots(x-s_{i-1})(x-s_{i+1})\ldots(x-s_q)}{(s_i-s_0)\ldots(s_i-s_{i-1})(s_i-s_{i+1})\ldots(s_i-s_q)}.$$

Ist $\varphi(x)$ Teiler von $f(x)$, so muß $\varphi(s_i)$ Teiler von $f(s_i)$ sein. Für $\varphi(s_i)$ kommen aber nur endlich viele Werte in Betracht, die einzeln durchdiskutiert werden sollen. Ist $m = 0$, so ist $f(s_i)$ eine ganze Zahl, deren endlich viele Teiler hingeschrieben werden können. Da der Satz nach 1a für Primkörper der Charakteristik p bereits bewiesen ist, so ist hiermit der Fall $m = l = 0$ vollständig erledigt.

Wir können also annehmen, daß die Zerlegung eines Polynoms in $[K][z_1 \ldots z_{m-1}]$ mit endlich vielen Schritten erreicht werden kann. $f(s_i)$ kann nun als Größe in $[K][z_1 \ldots z_m]$ aufgefaßt werden als Polynom in z_m mit Koeffizienten aus $[K][z_1 \ldots z_{m-1}]$, läßt sich also nach der Annahme mit endlich vielen Schritten in irreduzible Faktoren zerlegen.

2. Angenommen der Satz sei bereits für $l-1$ algebraische Erweiterungen bewiesen. α_l sei algebraisch in bezug auf $K(z_1 \ldots z_m \alpha_1 \ldots \alpha_{l-1})$. Durch die Substitution $x = y - u \cdot \alpha_l$, wo u eine Unbestimmte bedeutet, die zum Körper adjungiert wird und die nach 1. bei der Zerlegung nicht stört, erreicht man es, daß $f(y - u\alpha_l)$ sicher explizite von α_l abhängt. Man multipliziere $f(y - u\alpha_l)$ mit allen Polynomen, die hieraus hervorgehen, wenn α_l überall in f durch seine in bezug auf $K(z_1 \ldots z_m \alpha_1 \ldots \alpha_{l-1})$ konjugierten Elemente ersetzt wird. Das Produkt ist ein Polynom, dessen Koeffizienten in $K(z_1 \ldots z_m \alpha_1 \ldots \alpha_{l-1})$ liegen, das sich also nach Voraus-

setzung in diesem Körper mit endlich vielen Schritten in irreduzible Faktoren zerlegen läßt. Die größten gemeinsamen Teiler dieser Faktoren und des Polynoms $f(y - u\alpha_l)$ sind die Teiler von $f(y - u \cdot \alpha_l)$. Durch die Substitution $y = x + u\alpha_i$ erhält man daraus die gesuchten Teiler von $f(x)$, die sich also mit vielen Schritten berechnen lassen, q. e. d.

Der Fall, daß zum Primkörper unendlich viele transzendente Elemente adjungiert sind, läßt sich sofort auf den eben betrachteten Fall zurückführen. Das vorgelegte Polynom kann nämlich von diesen unendlich vielen Elementen nur endlich viele enthalten, und kein Teiler kann eins dieser transzendenten Elemente enthalten, das das Polynom selbst nicht enthält, wenn man sich zum Zerlegen wieder auf $[P][x]$ beschränkt. Es genügt also die Zerlegung vorzunehmen in dem Körper, der aus dem Primkörper entsteht durch Adjunktion der erforderlichen algebraischen Elemente und der endlich vielen im Polynom auftretenden transzendenten Elemente.

Anders wird es, wenn unendlich viele algebraische Elemente zum Primkörper adjungiert sind. Hier gilt es nicht, daß ein im Polynom $f(x)$ nicht vorkommendes algebraisches Element auch in den Teilern von f nicht vorkommen kann. Die Methoden des Kroneckerschen Satzes versagen hier. Es läßt sich aber eine Zerlegung des Polynoms in Linearfaktoren symbolisch in dem zu P gehörigen algebraisch abgeschlossenen Körper durchführen.

Zunächst ist es jedenfalls möglich, das Polynom in dem durch seine eignen Koeffizienten bestimmten Körper in Primfaktoren zu zerlegen, da unter den Koeffizienten nur endlich viele in bezug auf den Primkörper algebraische Elemente auftreten. Nach Steinitz kann man nun stets eine Nullstelle j einer solchen Primfunktion $g(x)$, für die also $g(j) = 0$ ist, symbolisch einführen, denn der durch Adjunktion eines solchen Symbols zum Koeffizientenkörper entstehende Bereich ist isomorph dem Restklassenkörper nach der Primfunktion, also selbst ein Körper. Wendet man dieses Verfahren endlich oft an, so erhält man eine Zerlegung des Polynoms in Linearfaktoren, zu der bekanntlich bereits ein endlicher Erweiterungskörper ausreicht. Ist dieser nicht selbst einem Unterkörper des vorgelegten Körpers, in dem zerlegt werden soll, isomorph, so gilt das jedenfalls von einem der endlich vielen Zwischenkörper, die den möglichen Zusammenfassungen in endlich viele Faktoren entsprechen.

§ 3.

Rechenoperationen der Idealtheorie.

Der Satz des § 3 soll zeigen, wie mit endlich vielen Schritten die einfachsten Rechenoperationen der Idealtheorie durchgeführt werden können.

Es handelt sich um das Bilden vom kleinsten gemeinschaftlichen Vielfachen und größten gemeinsamen Teiler, von Produkt und Quotient. Die Gesamtheit der Basiselemente zweier Ideale bildet eine Basis des größten gemeinsamen Teilers der beiden Ideale, die sich also sofort hinschreiben läßt. Ebenso ist die Basis des Produktes der beiden Ideale leicht zu finden. Sie besteht aus den sämtlichen Produkten von je einem Basiselement des einen Ideals mit einem des andern. Schwieriger ist die Bildung der Basis beim kleinsten gemeinschaftlichen Vielfachen und Quotienten. Die Methoden hierzu wird der Hilbertsche Satz liefern[7]).

Satz 2. Voraussetzung. *Es seien* f_{ij} *Polynome in* $x_1 \ldots x_n$ *mit Koeffizienten aus* P, *also Größen aus* $\mathsf{P}[x_1 \ldots x_n]$.

Behauptung. *Für das Gleichungssystem*

$$\begin{aligned} f_{11} z_1 + \ldots + f_{1s} z_s &= 0 \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ f_{t1} z_1 + \ldots + f_{ts} z_s &= 0 \end{aligned}$$

läßt sich mit endlich vielen Schritten ein vollständiges Lösungssystem berechnen, das ebenfalls aus Größen aus $\mathsf{P}[x_1 \ldots x_n]$ *besteht. Ist* q *der Maximalgrad der* f_{ij}, *so überschreiten die Polynome des vollständigen Lösungssystems nicht den Grad* $m(t, q, n)$; *dabei genügt* m *der Reduktionsformel* $m(t, q, 0) = 0$, $m(t, q, n) = q \cdot t + m(t^2 q, q, n-1)$. *Es wird also* $m(t, q, n) = \sum_{i=0}^{n-1} (q \cdot t)^{2^i}$.

Dabei ist unter einem vollständigen Lösungssystem ein System von Lösungen des Gleichungssystems zu verstehen, von dem jede andere Lösung linear mit Koeffizienten aus $\mathsf{P}[x_1 \ldots x_n]$ abhängt.

Beweis durch vollständige Induktion.

1. $n = 0$: die Koeffizienten f_{ij} und die gesuchten Lösungen z_i sind Konstante, Größen aus dem Körper P. Das Gleichungssystem läßt sich bekanntlich in diesem Fall mit endlich vielen Schritten auflösen, das Problem ist auf ein solches der Determinantentheorie zurückgeführt. Da überhaupt keine Unbestimmten auftreten, ist der Grad aller Polynome 0.

2. Angenommen der Satz sei für $n = r - 1$ $[r > 0]$ bereits bewiesen. Es sei $n = r$.

a) Das Gleichungssystem sei transformiert. Ohne Beschränkung der Allgemeinheit kann man voraussetzen, daß zwischen den Gleichungen keine linearen Beziehungen mehr bestehen, es ist also sicher $t \leqq s$. Ist $t = s$,

[7]) Auf die Möglichkeit der hier aus dem Hilbertschen Satz gezogenen Folgerungen weist bereits Macaulay hin. Math. Annalen 74.

so ist $z_1 = \ldots = z_s = 0$ die einzige Lösung, bildet also ein vollständiges Lösungssystem, der Satz ist für diesen Fall also bewiesen.

Es kann also angenommen werden $s > t$; t ist der Rang von

$$\left\| \begin{matrix} f_{11} \cdots f_{1s} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \\ f_{t1} \cdots f_{ts} \end{matrix} \right\|.$$

Man setze

$$D_{i_1 \ldots i_t} = \left| \begin{matrix} f_{1 i_1} \cdots f_{1 i_t} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \\ f_{t i_1} \cdots f_{t i_t} \end{matrix} \right|,$$

wobei $i_1 \ldots i_t$ irgendwelche t verschiedene Zahlen der Reihe $1 \ldots s$ bedeuten. Ohne Beschränkung der Allgemeinheit kann man annehmen, daß

$$D = D_{1 \ldots t} = \left| \begin{matrix} f_{11} \cdots f_{1t} \\ f_{t1} \cdots f_{tt} \end{matrix} \right| \neq 0$$

wird, und daß D vom höchsten Grad $\mu \leqq q \cdot t \leqq m(t, q, r)$ wird, der unter den $D_{i_1 \ldots i_t}$ überhaupt auftritt. Da das Gleichungssystem transformiert angenommen ist, kann D als regulär in x_1 angenommen werden, d. h. der Koeffizient von x_1^{μ} verschwindet in D nicht. Dann hat das gegebene Gleichungssystem die Lösungen:

$$z_1 = D_{t+1; 2 \ldots t}; \; \ldots z_t = D_{1 \ldots t-1; t+1}; \; z_{t+1} = D; \; z_{t+2} = \ldots = z_s = 0,$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$z_1 = D_{s; 2 \ldots t}; \; \ldots z_t = D_{1 \ldots t-1; s}; \; z_{t+1} = \ldots = z_{s-1} = 0; \; z_s = D,$$

die die ausgezeichneten Lösungen des Gleichungssystems heißen mögen. Die Polynome dieser Lösungen überschreiten den Grad μ nicht. Wegen der Regularität von D in x_1 läßt sich mit Hilfe dieser Lösungen aus jeder Lösung eine andere $\zeta_1 \ldots \zeta_s$ ableiten, für die gilt:

$$[\zeta_{t+1}]_1 < [D]_1 = \mu; \ldots [\zeta_s]_1 < \mu$$

und es gelten die Gleichungen:

$$l_1 = f_{11} \zeta_1 + \ldots + f_{1s} \zeta_s = 0,$$

$$\cdots\cdots\cdots\cdots$$

$$l_t = f_{t1} \zeta_1 + \ldots + f_{ts} \zeta_s = 0.$$

Bedeutet nun F_{ik} die zu f_{ik} gehörende $t-1$-reihige Unterdeterminante von D, so wird

$$0 = F_{11} l_1 + \ldots + F_{t1} l_t = D \zeta_1 + D_{t+1, 2 \ldots t} \zeta_{t+1} + \ldots + D_{s, 2 \ldots t} \zeta_s,$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$0 = F_{t1} l_1 + \ldots + F_{tt} l_t = D \zeta_t + D_{1 \ldots t-1; t+1} \zeta_{t+1} + \ldots + D_{1 \ldots t-1; s} \zeta_s.$$

Wegen

$$[D_{i_1 \dots i_t}]_1 \leqq \mu,$$
$$[\zeta_{t+\lambda}]_1 < \mu \quad \text{für} \quad \lambda = 1 \dots s - t,$$
$$[D]_1 = \mu$$

folgt daraus

$$[\zeta_i]_1 < \mu \quad \text{für} \quad i = 1 \dots t,$$

also gilt allgemein

$$[\zeta_i]_1 < \mu \quad \text{für} \quad i = 1 \dots s.$$

Es wird also

$$\zeta_1 = \xi_{11}^{(2)} x_1^{\mu-1} + \dots + \xi_{1\mu}^{(2)},$$
$$\dots\dots\dots\dots$$
$$\zeta_s = \xi_{s1}^{(2)} x_1^{\mu-1} + \dots + \xi_{1\mu}^{(2)}.$$

Dabei sind die $\xi_{ij}^{(2)}$ gemäß der Bezeichnung § 1, 6 Größen aus $\mathsf{P}[x_2 \dots x_r]$. Man setze diese Ausdrücke in die Gleichungen $l_1 = \dots = l_t = 0$ und ordne nach Potenzen von x_1. Die Koeffizienten dieser Potenzen, die nur noch von $x_2 \dots x_r$ abhängen, müssen dann einzeln verschwinden. Man erhält also Gleichungen der Form

$$\varphi_{11}^{(2)} \xi_{11}^{(2)} + \dots + \varphi_{1\sigma}^{(2)} \xi_{s\mu}^{(2)} = 0,$$
$$\dots\dots\dots\dots$$
$$\varphi_{\tau 1}^{(2)} \xi_{11}^{(2)} + \dots + \varphi_{\tau\sigma}^{(2)} \xi_{s\mu}^{(2)} = 0.$$

Dabei ist $[\varphi_{ij}] \leqq q$ und $\mu \cdot s = \sigma > \tau = \mu t \leqq q \cdot t^2$. Da für dieses Gleichungssystem $n = r - 1$ ist, so läßt sich nach Voraussetzung mit endlich vielen Schritten ein vollständiges Lösungssystem berechnen, dessen Elemente den Grad $m(q t^2, q, r-1)$ nicht überschreiten.

$\bar{\xi}_{11}^{(2)} \dots \bar{\xi}_{s\mu}^{(2)}$ sei eine Lösung dieses Gleichungssystems, dann ist

$$\bar{\xi}_1 = \bar{\xi}_{11}^{(2)} x_1^{\mu-1} + \dots + \xi_{1\mu}^{(2)},$$
$$\dots\dots\dots\dots$$
$$\bar{\xi}_s = \bar{\xi}_{s1}^{(2)} x_1^{\mu-1} + \dots + \xi_{s\mu}^{(2)}$$

Lösung des ursprünglichen Gleichungssystems, und umgekehrt läßt sich jede Lösung des vorgelegten Gleichungssystems modulo den ausgezeichneten Lösungen auf diese Form bringen. Zusammen mit den ausgezeichneten Lösungen bilden also die aus dem vollständigen Lösungssystem des von x_1 unabhängigen Gleichungssystems durch die angegebene Zusammensetzung mit Potenzen von x_1 gebildeten Lösungen ein vollständiges Lösungssystem des vorgelegten Gleichungssystems, das sich somit mit endlich vielen Schritten berechnen läßt. Diese Lösungen überschreiten den Grad $\mu + m(q t^2, q, r-1) \leqq q \cdot t + m(q t^2;\ q, r-1) = m(t, q, r)$ nicht.

b) Das Gleichungssystem sei nicht transformiert. Man transformiere es durch $x = U(x')$ und berechne nach a). das vollständige Lösungssystem

des transformierten Systems. Da nach Rücktransformation $x' = U^{-1}(x)$ die Koeffizienten des Gleichungssystems wieder von den Unbestimmten $u_{\mu\nu}$ unabhängig sind, so bilden die bei gleichen Potenzprodukten der $u_{\mu\nu}$ in den zurücktransformierten Lösungen stehenden Faktoren ein vollständiges Lösungssystem der vorgelegten Gleichungen, das sich also auch in diesem Fall mit endlich vielen Schritten berechnen läßt. Da beim Transformieren die Gradzahlen der Polynome nicht wachsen, so gilt auch hier die Gradbeschränkung, q. e. d.

Zusatz zu Satz 2. *Sind im Falle $t=1$ die Koeffizienten f_i der vorgelegten Gleichung homogen in $x_1 \dots x_\varrho$ $[0 \leqq \varrho \leqq n]$, so können die im vollständigen Lösungssystem auftretenden Polynome als homogen in $x_1 \dots x_\varrho$ angenommen werden, die Gradbeschränkung von Satz 2 bleibt bestehen.*

Beweis. $z_1 \dots z_s$ sei irgendeine Lösung der Gleichung, es wird also

$$f_1 z_1 + \dots + f_s z_s = 0.$$

Es sei

$$\begin{aligned} z_{11} + \dots + z_{1j_1} &= z_1 \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ z_{s1} + \dots + z_{sj_s} &= z_s \end{aligned}$$

die Aufspaltung dieser Polynome in Summanden, die in bezug auf $x_1 \dots x_\varrho$ homogen sind, derart, daß je zwei dieser Summanden in $x_1 \dots x_\varrho$ verschiedenen Grad haben. Dann ist $f_i \cdot z_{ik}$ homogen in bezug auf $x_1 \dots x_\varrho$, $f_i \cdot (z_{ik_1} + z_{ik_2})$ $[k_1 \neq k_2]$ aber nicht. Spaltet man also die Gleichung

$$f_1 z_1 + \dots + f_s z_s = 0$$

in Bestandteile auf, die in $x_1 \dots x_\varrho$ homogen, aber untereinander von verschiedenem Grad sind, so daß sie einzeln verschwinden müssen, so erhält man Gleichungen der Form

$$f_1 z_{1k_1} + \dots + f_s z_{sk_s} = 0.$$

Dabei gibt es so viele solche Gleichungen, daß jeder der Summanden $z_{ik} \begin{bmatrix} k = 1 \dots j_i \\ i = 1 \dots s \end{bmatrix}$ genau in einer Gleichung auftritt.

Die Systeme $z_{1k_1} \dots z_{sk_s}$ sind also Lösungen der Gleichung. Von ihnen hängt die Lösung $z_1 \dots z_s$ linear ab; sie ergibt sich durch Summation über diese Lösungen. Durch entsprechende Aufspaltung der in einem vollständigen Lösungssystem auftretenden Lösungen, die sich nach dem angegebenen Verfahren mit endlich vielen Schritten durchführen läßt, erhält man ein vollständiges Lösungssystem der Gleichung, das aus in $x_1 \dots x_\varrho$ homogenen Polynomen besteht und denselben Maximalgrad hat, wie das ursprüngliche Lösungssystem, q. e. d.

Anwendung von Satz 2.

1. *Berechnung des kleinsten gemeinsamen Vielfachen* $[\mathfrak{a}, \mathfrak{b}]$ zweier Ideale $\mathfrak{a} = (f_1 \dots f_t)$ und $\mathfrak{b} = (g_1 \dots g_s)$ mit endlich vielen Schritten.

Es ist

$$c \equiv 0 ([\mathfrak{a}, \mathfrak{b}])$$

dann und nur dann, wenn

$$c \equiv 0 (\mathfrak{a}) \quad \text{und} \quad c \equiv 0 (\mathfrak{b})$$

gilt, d. h. wenn

$$c = d_1 f_1 + \dots + d_t f_t = e_1 g_1 + \dots + e_s g_s$$

ist. Es wird also in diesem Fall

$$d_1 f_1 + \dots + d_t f_t - e_1 g_1 - \dots - e_s g_s = 0.$$

Nach Satz 2 läßt sich ein vollständiges Lösungssystem dieser Gleichung berechnen.

$$\begin{matrix} d_{11} \dots d_{1t} e_{11} \dots e_{1s} \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ d_{k1} \dots d_{kt} e_{k1} \dots e_{ks} \end{matrix}$$

sei ein solches. Dann ist

$$\begin{matrix} c_1 = d_{11} f_1 + \dots + d_{1t} f_t = e_{11} g_1 + \dots + e_{1s} g_s \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ c_k = d_{k1} f_1 + \dots + d_{kt} f_{kt} = e_{k1} g_1 + \dots + e_{ks} g_s \end{matrix}$$

eine Basis von $[\mathfrak{a}, \mathfrak{b}]$. Es wird also $[\mathfrak{a}, \mathfrak{b}] = (c_1 \dots c_k)$.

2. *Berechnung des Quotienten* $\mathfrak{a} : \mathfrak{b}$.

Bekanntlich ist: $\mathfrak{a} : \mathfrak{b} = [\mathfrak{a} : (g_1) \dots \mathfrak{a} : (g_s)]$.

Nun ist

$$c \equiv 0 (\mathfrak{a} : (g_j))$$

dann und nur dann, wenn

$$c \cdot g_j = d_1 f_1 + \dots + d_t f_t$$

wird, wenn also

$$c \cdot g_j - d_1 f_1 - \dots - d_t f_t = 0$$

ist.

Nach Satz 2 läßt sich ein vollständiges Lösungssystem dieser Gleichung berechnen. $c_{j1} \dots c_{jm_j}$ seien die darin zu g_j gehörenden Faktoren. Dann ist

$$\mathfrak{a} : (g_j) = (c_{j1} \dots c_{jm_j}).$$

Die Basis von $\mathfrak{a} : \mathfrak{b} = [\mathfrak{a} : (g_1) \dots \mathfrak{a} : (g_s)]$ läßt sich nach 1 ebenfalls mit endlich vielen Schritten berechnen.

§ 4.

Gradbeschränkung bei formalen Teilbarkeitssätzen.

Satz 3 liefert nun ein Kriterium, mit Hilfe dessen man mit endlich vielen Schritten feststellen kann, ob zwei Ideale durcheinander teilbar sind oder nicht[7a]).

Satz 3. Voraussetzung. $\mathfrak{M} = (l_1 \dots l_t)$ *sei ein Modul aus Linearformen in* $z_1 \dots z_s$, *deren Koeffizienten Polynome* $f_{ij}(x_1 \dots x_n)$ *aus* $\mathsf{P}[x_1 \dots x_n]$ *sind, die von* $z_1 \dots z_s$ *unabhängig sind. Es sei* $[f_{ij}] \leqq q$ *und*

$$\begin{aligned} l_1 &= f_{11} z_1 + \dots + f_{1s} z_s, \\ &\dots\dots\dots\dots \\ l_t &= f_{t1} z_1 + \dots + f_{ts} z_s. \end{aligned}$$

Es sei $l \equiv 0\,(\mathfrak{M})$, *also*

$$l = a_1 l_1 + \dots + a_t l_t.$$

Behauptung. *Diese Darstellung kann so gewählt werden, daß*

$$[a_i] \leqq [l] + 2\,m(t; q; n).$$

Dabei ist $m(t, q, n)$ *genau wie in Satz 2 definiert.*

Beweis durch vollständige Induktion.

1. $n = 0$. In diesem Fall ist der Satz evident, da alle vorkommenden Polynome in den x vom Grade 0 sind. Es ist also sicher $[a_i] = [l] + 0 = 0$.

2. Angenommen der Satz sei für $n = r - 1$ bereits bewiesen. Es sei $n = r$; p sei der Rang von

$$\left\| \begin{matrix} f_{11} \dots f_{1s} \\ f_{t1} \dots f_{ts} \end{matrix} \right\|.$$

Sicher ist $p \leqq t$. Wie in Satz 2 setze man

$$\begin{vmatrix} f_{1i_1} \dots f_{1i_p} \\ f_{pi_1} \dots f_{pi_p} \end{vmatrix} = D_{i_1 \dots i_p}$$

und nehme an

$$\begin{vmatrix} f_{11} \dots f_{1p} \\ \dots\dots \\ f_{p1} \dots f_{pp} \end{vmatrix} = D_{1 \dots p} = D \neq 0.$$

[7a]) Ein solches Kriterium bringt bereits König durch die Auflösung der inhomogenen Gleichung $f_1 z_1 + \dots + f_s z_s = f$ unter Benutzung der Auflösbarkeit der homogenen Gleichung, wobei der Induktionssohluß gemäß der Anmerkung 4 modifiziert werden muß. Die in Satz 3 berechneten für das Weitere wichtigen Gradbeschränkungen bringt König nicht.

a) Angenommen $\mathfrak{M}$ sei transformiert, dann kann D als regulär in x_1 angenommen werden. Dann ist

$$[D]_1 = [D] \leqq q \cdot t.$$

Bedeutet F_{ij} die zu f_{ij} gehörende $p-1$-reihige Unterdeterminante von D, so enthält $\mathfrak{M}$ die Formen

$$\begin{aligned} m_1 &= F_{11} l_1 + \ldots + F_{1p} l_p \equiv 0 \,(\mathfrak{M}), \\ &\cdots\cdots\cdots\cdots \\ m_p &= F_{p1} l_1 + \ldots + F_{pp} l_p \equiv 0 \,(\mathfrak{M}) \end{aligned}$$

und zwar ist

$$\begin{aligned} m_1 &= D z_1 + D_{p+1,2\ldots p} z_{p+1} + \ldots + D_{s,2\ldots p} z_s \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ m_p &= D z_p + D_{1\ldots p-1,\,p+1} z_{p+1} + \ldots + D_{1\ldots p-1,\,s} z_s . \end{aligned}$$

Es wird $[F_{ik}] \leqq (t-1)\cdot q$; $[l_i] \leqq q$ also $[m_i] \leqq q \cdot t$, und zwar gilt das für jeden Term der Darstellung durch die l.

Es sei nun $g(z) = g_1 z_1 + \ldots + g_s z_s$ eine Linearform in den z mit Koeffizienten aus $\mathsf{P}[x_1 \ldots x_r]$. Wegen der Regularität von D in x_1 gibt es Polynome G_i und j_i, so daß

$$g_i = G_i + D j_i$$

wird für $i = 1 \ldots p$. Dabei wird

$$[G_i]_1 < [D]$$

und es läßt sich zeigen, daß

$$[j_i] \leqq [g_i] \leqq [g]$$

wird.

Zum Beweis nehme man an $[j_i] > [g_i]$. Es sei $j_i = j_{i1} + \ldots + j_{ik_i}$ die Aufspaltung von j_i in homogene Summanden verschiedenen Grades und zwar sei $[j_{i1}] = [j_i]$. Es sei $j_{i1}^{(2)}(x_2 \ldots x_r) \not\equiv 0$ der Koeffizient der höchsten in j_{i1} auftretenden Potenz von x_1. Es wird also $j_{i1} = j_{i1}^{(2)} \cdot x_1^{\varkappa} + \ldots$ und $[j_{i1}^{(2)}] = [j_i] - \varkappa$. Wegen der Regularität von D in x_1 ist

$$D = b\, x_1^{[D]} + \ldots .$$

Dabei ist $b \neq 0$ eine Größe aus P. Es wird also

$$j_i D = f^{(2)} \cdot x_1^{\varkappa + [D]} + \ldots .$$

Dabei ist

$$f^{(2)} = b\, j_{i1}^{(2)} + \ldots$$

Glieder niedrigeren Grades. Also ist $f^{(2)} \neq 0$ und $[f^{(2)}] = [j_i] - \varkappa$. Da $[G_i]_1 < [D]$ ist, so ist $f^{(2)}$ in g_i der Koeffizient von $x_1^{\varkappa+[D]}$, und es ist $[g_i] \geqq [x_1^{\varkappa+[D]} \cdot f^{(2)}] = [D] + [j_i] > [D] + [g_i] \geqq [g_i]$, die Voraussetzung

$[j_i] > [g_i]$ hat also zu einem Widerspruch geführt. Es ist also, wie behauptet wurde, $[j_i] \leqq [g_i]$.

Man kann setzen

$$g(z) = G(z) + \sum_{i=1}^{p} m_i j_i.$$

Dabei ist

$$G(z) = G_1 z_1 + \ldots + G_p z_p + G_{p+1} z_{p+1} + \ldots + G_s z_s,$$

und es wird

$$[\sum_{i=1}^{p} m_i j_i] \leqq [g] + q \cdot t \leqq [g] + m(t, q, r),$$

und zwar gilt das für jeden Term der Darstellung durch die l. Ist $g(z) \equiv 0 (\mathfrak{M})$, so ist wegen $m_i \equiv 0 (\mathfrak{M})$ auch $G(z) \equiv 0 (\mathfrak{M})$ und es braucht nach dem Vorigen der Satz nur noch für $G(z)$ bewiesen zu werden.

Aus

$$G(z) \equiv 0 (\mathfrak{M})$$

folgt

$$G(z) = a_1 l_1 + \ldots + a_t l_t,$$

es wird also

$$G_i = a_1 f_{i1} + \ldots + a_t f_{it}.$$

Da p der Rang von $\mathfrak{M}$ ist, so ist $l_{p+\lambda}$ $[0 < \lambda \leqq t - p]$ linear abhängig von $l_1 \ldots l_p$, falls $\frac{1}{D}$ als Multiplikator zugelassen wird; also ist

$$D \cdot l_{p+\lambda} \equiv 0 (l_1 \ldots l_p).$$

Wegen der Regularität von D in bezug auf x_1 können deshalb die a so gewählt werden, daß

$$[a_{p+\lambda}]_1 < [D] \quad \text{wird für} \quad 0 < \lambda \leqq t - p.$$

Nun ist

$$\sum_{i=1}^{p} G_i F_{ik} = D \cdot a_k + \sum_{\tau=p+1}^{t} a_\tau \sum_{\pi=1}^{p} f_{\pi\tau} F_{\pi k}.$$

Dabei ist

$$[\sum f_{\pi\tau} F_{\pi k}] \leqq q \cdot t,$$
$$[a_\tau]_1 \leqq [D], \quad \text{für} \quad \tau = p+1 \ldots t,$$
$$[G_i]_1 \leqq [D], \quad \text{für} \quad i = 1 \ldots p,$$
$$[F_{ik}] \leqq q(t-1),$$

also wird

$$[a_k]_1 \leqq q \cdot t, \quad \text{für} \quad k = 1 \ldots t,$$

d. h.

$$[a_k]_1 \leqq 2\, m(t; q; 1).$$

Für $r = 1$ ist der Satz damit bewiesen. Es sei $r > 1$; dann ist

$$G(z) \equiv 0 (\mathfrak{B}),$$

wobei

$$\mathfrak{B} = (l_1; x_1 l_1 \ldots x_1^{q \cdot t} l_1; l_2; \ldots x_1^{q \cdot t} l_t)$$

ein Modul aus Linearformen in $z_1; x_1 z_1 \dots x_1^{q \cdot t} z_1 \dots x_1^{q \cdot t} z_s$ ist mit Koeffizienten aus $\mathsf{P}[x_2 \dots x_r]$. Die Anzahl T der Basiselemente von $\mathfrak{B}$ ist $q \cdot t^2$. Da die Koeffizienten von $\mathfrak{B}$ nur von $r-1$ Variablen abhängen, so gibt es nach Voraussetzung eine Darstellung

$$G(z) = a_1^{(2)} l_1 + \dots + a_T^{(2)} x_1^{q \cdot t} l_t,$$

wobei

$$[a_i^{(2)}] \leqq [G] + 2m(qt^2; q; r-1)$$

gilt. Wegen

$$g = G + \sum_{i=1}^{p} m_i j_i$$

und

$$[\sum m_i j_i] \leqq [g] + q \cdot t$$

ist nun

$$[G] \leqq [g] + q \cdot t.$$

Es wird also

$$[a_i^{(2)}] \leqq [g] + q \cdot t + 2m(q \cdot t^2; q; r-1).$$

Ordnet man die Darstellung von $G(z)$ nach den l

$$G(z) = a_1 l_1 + \dots + a_t l_t,$$

so wird

$$[a_i] \leqq \max [a_k^{(2)}] + q \cdot t,$$

d. h. es wird

$$[a_i] \leqq [g] + 2q \cdot t + 2m(q \cdot t^2; q; r-1) = [g] + 2m(t; q; r).$$

b) $\mathfrak{M}$ sei nicht transformiert. Der Satz gilt für den entsprechenden transformierten Modul. Da sich beim Rückgängigmachen der Transformation die Gradzahlen nicht erhöhen, gilt der Satz auch im nichttransformierten Modul, q. e. d.

Anwendung von Satz 3.

Kriterium für die Teilbarkeit zweier Ideale durcheinander.

Setzt man $s = 1$ und läßt das in allen Elementen von $\mathfrak{M}$ als Faktor auftretende z_1 weg, so geht $\mathfrak{M}$ über in ein Ideal $\mathfrak{m} = (f_1 \dots f_t)$ aus Polynomen in $x_1 \dots x_n$, und der Satz besagt: Ist $g \equiv 0 (\mathfrak{m})$, so gibt es eine Darstellung

$$g = g_1 f_1 + \dots + g_t f_t,$$

wobei

$$[g_i] \leqq [g] + 2m(t, q, n)$$

ist. Setzt man also für die g_i Polynome vom Grad $[g] + m(t, q, n)$ an, deren Koeffizienten Unbestimmte sind, so müssen die Gleichungen, die aus der Gleichung $g = \sum_{i=1}^{t} f_i g_i$ durch Koeffizientenvergleichung entstehen,

auflösbar sein. Sind sie umgekehrt auflösbar, so ist $g \equiv 0\,(\mathfrak{m})$. Das fragliche Gleichungssystem, auf dessen Auflösbarkeit es also ankommt, ist nun linear in den Unbekannten. Nach den Methoden der Determinantentheorie läßt sich seine Auflösbarkeit also mit endlich vielen Schritten entscheiden. Für jedes einzelne Polynom aus $\mathsf{P}[x_1 \dots x_n]$ kann man also mit endlich vielen Schritten entscheiden, ob es durch $\mathfrak{m}$ teilbar ist oder nicht. Da nun für die Teilbarkeit eines Ideals durch ein anderes notwendig und hinreichend ist, daß die Basiselemente des ersten durch das zweite teilbar sind, so ist hiermit bereits ein Kriterium für die Teilbarkeit eines Ideals durch ein anderes geliefert.

Später wird es wichtig werden, daß man ein Gradüberschreiten gänzlich ausschließen kann. Satz 4 wird zeigen, daß es in der Tat eine Idealbasis gibt, für die das möglich ist.

Satz 4. *Zu jedem Ideal* $\mathfrak{m} = (f_1 \dots f_t)$ *gibt es eine ausgezeichnete Idealbasis* $f_{\varrho 1} \dots f_{\varrho t_\varrho}$ $[\varrho = 1 \dots n]$ *derart, daß es zu jedem* $g \equiv 0\,(\mathfrak{m})$ *eine Darstellung*

$$g = \sum_{i=1}^{t_\varrho} g_i f_{\varrho i}$$

gibt, wobei

$$[g_i]_\varrho = [g]_\varrho - [f_{\varrho i}]_\varrho$$

wird für $g_i \neq 0$. *Diese Basis läßt sich mit endlich vielen Schritten berechnen, es wird* $[f_{\varrho i}] \leqq m(1; q; n) = \sum_{i=0}^{n-1} q^{2^i}$.

Beweis: Man setze

$$\bar{f}_\tau(x_0 x_1 \dots x_n) = x_0^{[f_\tau]_\varrho} f_\tau\left(\frac{x_1}{x_0} \dots \frac{x_\varrho}{x_0}; x_{\varrho+1} \dots x_n\right),$$

so daß $\bar{f}_\tau$ in $x_0 \dots x_\varrho$ homogen wird. Es sei $g \equiv 0\,(\mathfrak{m})$,

$$\bar{g}(x_0 x_1 \dots x_n) = x_0^{[g]_\varrho} g\left(\frac{x_1}{x_0} \dots \frac{x_\varrho}{x_0}; x_{\varrho+1} \dots x_n\right).$$

Nach Satz 3 gibt es eine Darstellung

$$g = c_1 f_1 + \dots + c_t f_t,$$

so daß

$$[c_i] \leqq [g] + 2m(t, q, n)$$

ist. Folglich wird

$$x_0^k \bar{g} = \sum_{i=1}^{t} x_0^{k_i} \bar{c}_i \bar{f}_i.$$

Dabei sind die $\bar{c}_i$ analog den $\bar{f}_i$ und $\bar{g}_i$ gebildet, die k_i können so gewählt werden, daß für mindestens ein i der Exponent $k_i = 0$ wird, und es wird

$$k \leqq q + 2m(t, q, n).$$

Also gilt

$$x_0^{2m+q} \bar{g} \equiv 0\,(\bar{f}_1 \dots \bar{f}_t) \quad \text{in} \quad P[x_0 x_1 \dots x_n].$$

Gilt umgekehrt diese Kongruenz, so erhält man, wenn man $x_0 = 1$ setzt, $g \equiv 0(\mathfrak{m})$.

Man bilde also nach den in Satz 2 angegebenen Methoden ein vollständiges Lösungssystem der Gleichung:

$$x_0^{2m+q}\mathfrak{X} - \bar{c}_1\bar{f}_1 - \ldots - \bar{c}_t\bar{f}_t = 0,$$

das nach dem Zusatz zu Satz 2 als homogen in $x_0 x_1 \ldots x_\varrho$ angenommen werden kann. In ihm sei $\mathfrak{X} = \bar{f}_{\varrho 1} \ldots \mathfrak{X} = \bar{f}_{\varrho t_\varrho}$. Es ist also

$$[\bar{f}_{\varrho i}] \leqq m(1, q, n) = \sum_{i=0}^{n-1} q^{2^i}.$$

Es sei

$$g \equiv 0(\mathfrak{m}),$$

so folgt

$$\bar{g} = \sum_{i=1}^{t_\varrho} \bar{g}_i \bar{f}_{\varrho i},$$

dabei können die $\bar{g}_i$ ohne Beschränkung der Allgemeinheit als homogen in $x_1 \ldots x_\varrho$ angenommen werden. Da in dieser Gleichung alle Glieder homogen in $x_0 x_1 \ldots x_\varrho$ sind, so können die $\bar{g}_i$ so gewählt werden, daß

$$[\bar{g}_i]_\varrho = [\bar{g}]_\varrho - [\bar{f}_{\varrho i}]_\varrho$$

wird, falls $g_i \neq 0$ ist.

Setzt man nun $x_0 = 1$, und geht dabei $f_{\varrho i}$ aus $\bar{f}_{\varrho i}$ hervor, so wird

$$\mathfrak{m} = (f_{\varrho 1} \ldots f_{\varrho t_\varrho}),$$

es ist

$$[f_{\varrho i}] \leqq \sum_{i=0}^{n-1} q^{2^i},$$

und aus

$$g \equiv 0(\mathfrak{m})$$

folgt

$$g = \sum_{i=1}^{t_\varrho} g_i f_{\varrho i},$$

wobei

$$[g_i] = [g]_\varrho - [f_{\varrho i}]_\varrho$$

wird für $g_i \neq 0$, q. e. d.

§ 5.

Der Hentzeltsche Nullstellensatz.

Der Hentzeltsche Nullstellensatz bringt im Gegensatz zu dem rein formalen Teilbarkeitskriterium von Satz 3 ein Kriterium, das angibt, wie stark ein Polynom in den Nullstellen eines Ideals verschwinden muß, um durch das Ideal teilbar zu sein. Zum Beweis dieses Satzes sind drei Hilfssätze nötig.

In den Hilfssätzen muß vorausgesetzt werden, daß der den auftretenden Idealen und Moduln zugrunde gelegte Körper $\overline{P}$ [§ 1, 1] unendlich viele Elemente besitzt. Diese Bedingung ist sicher erfüllt, wenn man $\overline{P}$ durch $\overline{P}(s)$, wo s transzendent in bezug auf $\overline{P}$ ist, ersetzt. In den Hilfssätzen soll deshalb $\overline{P}$ unendlich viele Elemente enthalten. Es wird sich zeigen, daß die Adjunktion von s für den Hentzeltschen Nullstellensatz keine Einschränkung bedeutet.

Hilfssatz 1. Voraussetzung. *Es sei* $\mathfrak{M} = (l_1 \dots l_t)$ *ein Modul aus Linearformen*

$$\begin{aligned} l_1 &= f_{11} z_1 + \dots + f_{1s} z_s \\ &\cdots\cdots\cdots \\ l_t &= f_{t1} z_1 + \dots + f_{ts} z_s \end{aligned}$$

$[f_{ij}] \leqq q$; *es sei* p *der Rang von* $\mathfrak{M}$.

Behauptung. *Nach einer linearen homogenen Transformation* $x = U'(x')$ *der* $x_1 \dots x_n$ *mit Transformationskoeffizienten aus* $\overline{P}$, *die eine nicht verschwindende Determinante besitzen, gilt: Besteht* $\mathfrak{G}_n$ *aus der Gesamtheit der Linearformen* g, *für die es ein nur von* x'_n *abhängendes Polynom* $k(x'_n) \neq 0$ *gibt, so daß* $k(x'_n) \cdot g \equiv 0 (\mathfrak{M})$, *so gibt es ein nur von* x'_n *abhängendes Polynom* $K(x'_n) \neq 0$, *so daß*

1. $K(x'_n)\, \mathfrak{G}_n \equiv 0 (\mathfrak{M})$,
2. $[K(x'_n)] \leqq M(t, q, n)$

wird. Dabei ist

$$M(t, q, 1) = q \cdot t,$$

$$M(t, q, n) = M(q \cdot t^2, q, n-1).$$

Es ist also

$$M(t, q, n) = (q \cdot t)^{(2^{(n-1)})}.$$

Beweis durch vollständige Induktion.

1. $n = 1$. $\mathfrak{G}_1 = \mathfrak{G}$ ist der Grundmodul von $\mathfrak{M}$.[8]) Es sei

$$D = \begin{vmatrix} f_{11} \cdots f_{1p} \\ f_{p1} \cdots f_{pp} \end{vmatrix} \neq 0.$$

Nach H. N. Satz 3 ist

$$D \cdot \mathfrak{G} \equiv 0 (\mathfrak{M})$$

und es ist

$$[D]_1 \leqq [D] \leqq q \cdot t = M(t, q, 1).$$

2. Angenommen der Satz sei bereits für $n = r - 1$ bewiesen. Es sei $n = r > 1$. Da $\overline{P}$ unendlich viele Elemente enthält, kann man durch eine Transformation, die den in der Behauptung genannten Bedingungen genügt,

[8]) Die Definition des Grundmoduls ist gegeben N. § 1, 5.

stets erreichen, daß D regulär in x_1' wird. Zur Vereinfachung der Schreibweise sollen im folgenden die Akzente an den x wieder weggelassen werden. Es sei

$$k(x_r)\cdot g \equiv 0\,(\mathfrak{M}).$$

Wie in Satz 3 werde gesetzt

$$g = g_1 z_1 + \ldots + g_s z_s$$

und

$$g_i = G_i + D j_i,$$

so daß

$$[G_i]_1 \leqq [D] \leqq q\cdot t,$$

$$[j_i] \leqq [g_i] \leqq [g]$$

ist. Dann wird

$$g = G + \sum_{i=1}^{p} m_i j_i;$$

dabei haben die m_i dieselbe Bedeutung wie in Satz 3. Wegen $m_i \equiv 0\,(\mathfrak{M})$ wird

$$k(x_r)\,G \equiv 0\,(\mathfrak{M}).$$

Dabei ist

$$[k(x_r)\,G_i]_1 \leqq q\cdot t \quad \text{für} \quad i = 1 \ldots p.$$

Es sei

$$k(x_r)\,G = a_1 l_1 + \ldots + a_t l_t.$$

Dann kann man genau wie in Satz 3 zeigen

$$[a_i] \leqq q\cdot t \quad \text{für} \quad i = 1 \ldots t.$$

Es wird also

$$k(x_r)\,G \equiv 0\,(\mathfrak{B}),$$

wo $\mathfrak{B}$ wieder den Linearformenmodul $(l_1 \ldots l_t \ldots x_1^{q\cdot t} l_t)$, dessen Koeffizienten Polynome in $x_2 \ldots x_r$ sind, bedeutet. Nach Voraussetzung gibt es also nach einer Transformation von $x_2 \ldots x_r$, die mit der ersten zusammengesetzt werden kann, ein von der Wahl von g unabhängiges Polynom $K(x_r)$, so daß

$$K(x_r)\,G \equiv 0\,(\mathfrak{B})$$

und

$$[K(x_r)] \leqq M(q\cdot t^2, q, r-1)$$

wird. Es folgt ferner

$$K(x_r)\,G \equiv 0\,(\mathfrak{M}),$$

also auch

$$K(x_r)\,g \equiv 0\,(\mathfrak{M}),$$

also auch

$$K(x_r)\,\mathfrak{G}_r \equiv 0\,(\mathfrak{M})$$

und es ist

$$[K(x_r)] \leqq M(q\cdot t^2, q, r-1) = M(t, q, r)$$

q. e. d.

Zusatz 1 zu Hilfssatz 1. *Ist $\mathfrak{M}$ transformiert, so gilt die Behauptung, ohne daß die spezielle Transformation durchgeführt ist.*

Beweis. $\mathfrak{M}$ sei durch $y = U(x)$ aus $\overline{\mathfrak{M}}$ entstanden. Durch $x = U'(x')$ geht $\mathfrak{M}$ über in $\mathfrak{M}'$. $\mathfrak{M}'$ ist also aus $\overline{\mathfrak{M}}$ entstanden durch die zusammengesetzte Transformation $y = UU'(x') = V(x')$. Zwischen den Transformationsmatrizes bestehen also die Gleichungen

$$V = U \cdot U', \qquad U = VU'^{-1},$$

denn da U' eine nicht verschwindende Determinante hat, ist die Transformation eindeutig umkehrbar. Nach diesen Gleichungen können die Elemente von V und die von U gegenseitig durcheinander linear mit Koeffizienten aus $\overline{\mathsf{P}}$ ausgedrückt werden. Mit den Elementen von U sind also auch die von V Unbestimmte, und die Körper $\overline{\mathsf{P}}(u)$ und $\overline{\mathsf{P}}(v)$ stimmen überein. $\mathfrak{M}'$ ist also ebenfalls der zu $\overline{\mathfrak{M}}$ gehörige transformierte Modul, $\mathfrak{M}'$ ist also mit $\mathfrak{M}$ isomorph und unterscheidet sich von ihm nur durch die Bezeichnungsweise. Ersetzt man in $\mathfrak{M}'$ die x' durch die x und V durch U, so geht $\mathfrak{M}'$ in $\mathfrak{M}$ über. Da der Satz für $\mathfrak{M}'$ bewiesen ist, gilt er also auch für $\mathfrak{M}$, q. e. d.

Zusatz 2 zu Hilfssatz 1. *Im Spezialfall $s = 1$ liefert der Satz für transformierte Ideale eine obere Schranke für den Grad des Elementarteilers n-ter Stufe.*

Beweis. In diesem Fall geht nämlich $\mathfrak{M}$ über in ein Ideal $\mathfrak{m}$, da der in jedem Element auftretende Faktor z_1 als unwesentlich gestrichen werden kann. $\mathfrak{M}$ und somit auch $\mathfrak{m}$ sei transformiert. Dann geht $\mathfrak{G}_n$ über in das $n-1$-te Grundideal $\mathfrak{g}_{n-1}$ von $\mathfrak{m}$. Ist nun $E(x_n)$ Elementarteiler n-ter Stufe von $\mathfrak{m}$, so ist $E(x_n)$ der größte gemeinsame Teiler aller $K(x_n)$, für die gilt

$$K(x_n)\mathfrak{g}_{n-1} \equiv 0\,(\mathfrak{m}).$$ [9])

Nach Hilfssatz 1 und dem ersten Zusatz ist also

$$[E(x_n)] \leqq M(t, q, n).$$

Hilfssatz 2. Voraussetzung. *Es seien $\xi_{\varrho+1} \ldots \xi_n$ irgendwelche in einem Erweiterungskörper von $\overline{\mathsf{P}}$ gelegene Größen, sie mögen dem Körper $\overline{\mathsf{P}}$ adjungiert werden. Es seien definiert die Ideale*

$$\mathfrak{m} = (f_1 \ldots f_t), \quad q \geqq [f_i] \quad \text{für} \quad i = 1 \ldots t,$$
$$\mathfrak{d} = ((x_{\varrho+1} - \xi_{\varrho+1})^{e_{\varrho+1}}, \ldots, (x_n - \xi_n)^{e_n}),$$
$$\mathfrak{a} = (\mathfrak{m}, \mathfrak{d}).$$

[9]) Siehe N. § 1, 5.

Behauptung. *Nach einer linearen homogenen Transformation* $x = U'(x')$ *der Form*

$$\begin{aligned} x_1 &= u_{11}\,x_1' + \ldots + u_{1\varrho}\,x_\varrho', \\ &\cdots\cdots\cdots\cdots \\ x_\varrho &= u_{\varrho 1}\,x_1' + \ldots + u_{\varrho\varrho}\,x_\varrho', \\ x_{\varrho+1} &= \qquad\qquad\qquad x_{\varrho+1}', \\ &\cdots\cdots\cdots\cdots \\ x_n &= \qquad\qquad\qquad x_n' \end{aligned}$$

mit Koeffizienten aus $\overline{\mathsf{P}}$, *die eine nicht verschwindende Determinante besitzen, gilt: Bedeute* $\mathfrak{g}_\varrho$ *die Gesamtheit der Polynome* g, *für die es ein nur von* x_ϱ' *abhängendes Polynom* $k(x_\varrho')$ *gibt, so daß* $k(x_\varrho')\cdot g \equiv 0\,(\mathfrak{a})$, $k \neq 0$, *so gibt es ein nur von* x_ϱ' *abhängendes Polynom* $K(x_\varrho')$, *so daß*

1. $K(x_\varrho')\cdot\mathfrak{g}_\varrho \equiv 0\,(\mathfrak{a})$,
2. $[K(x_\varrho')] \leqq N(t, q, \varrho, \prod_{i=\varrho+1}^{n} e_i)$

wird. Dabei ist

$$N(t, q, \varrho, \prod_{i=\varrho+1}^{n} e_i) = M(t\cdot \prod_{i=\varrho+1}^{n} e_i, q, \varrho) = (q\cdot t\cdot \prod_{i=\varrho+1}^{n} e_i)^{(2^\varrho - 1)}.$$

Beweis. Es seien X_μ $[\mu = 1 \ldots S,\ S = \Pi e_i]$ die Potenzprodukte von $(x_{\varrho+1} - \xi_{\varrho+1}), \ldots, (x_n - \xi_n)$, bei denen der Exponent von $(x_i - \xi_i)$ kleiner als e_i ist. Man setze

$$f_\varkappa X_\mu \equiv \sum_{\sigma=1}^{S} X_\sigma f_{\sigma\tau_{\varkappa\mu}}(x_1 \ldots x_\varrho)\ (\mathfrak{d})$$

$$\varkappa = 1 \ldots t, \qquad \mu = 1 \ldots S, \qquad \tau_{\varkappa\mu} = 1 \ldots t\cdot S.$$

Ist i eine der Zahlen $1 \ldots t\cdot S$, so sei

$$l_i = X_1 f_{1i} + \ldots + X_S f_{Si}.$$

Dann ist $\mathfrak{M} = (l_1 \ldots l_{t\cdot S})$ der Linearformenmodul, in den $\mathfrak{m}$ modulo $\mathfrak{d}$ übergeht. $\mathfrak{M}$ werde so transformiert, wie es in Hilfssatz 1 angegeben ist. Der Akzent an den x werde wieder weggelassen. Da die Koeffizienten in $\mathfrak{M}$ nur Polynome in $x_1 \ldots x_\varrho$ sind, bezieht sich die Transformation zunächst nur auf $x_1 \ldots x_\varrho$. Sie kann durch die identische Transformation der $x_{\varrho+1} \ldots x_n$ zu $x = U'(x')$ erweitert werden. Nach Hilfssatz 1 gibt es dann ein nur von x_ϱ abhängendes Polynom $K(x_\varrho)$, so daß

$$K(x_\varrho)\cdot\mathfrak{G}_\varrho \equiv 0\,(\mathfrak{M})$$

und

$$[K(x_\varrho)] \leqq M(t\cdot S, q, \varrho) = N(t, q, \varrho, S)$$

wird. Faßt man die Elemente von $\mathfrak{G}_\varrho$ und $\mathfrak{M}$ wieder auf als Polynome in $x_1 \ldots x_n$, so gilt

$$(\mathfrak{G}_\varrho, \mathfrak{d}) = (\mathfrak{g}_\varrho, \mathfrak{d}),$$
$$(\mathfrak{M}, \mathfrak{d}) = (\mathfrak{m}, \mathfrak{d}) = \mathfrak{a}.$$

Es wird also

$$K(x_\varrho)(\mathfrak{g}_\varrho, \mathfrak{d}) \equiv 0(\mathfrak{a}).$$

Also gilt erst recht

$$K(x_\varrho)\mathfrak{g}_\varrho \equiv 0(\mathfrak{a})$$

q. e. d.

Zusatz zu Hilfssatz 2. *Ist* $\mathfrak{m}$ *transformiert, so gilt die Behauptung, ohne daß die spezielle Transformation durchgeführt ist.*

Beweis. $\mathfrak{m}$ sei durch die Transformation $y = U(x)$ aus $\overline{\mathfrak{m}}$ entstanden. Durch $x = U'(x')$ gehe $\mathfrak{m}'$, $\mathfrak{a}'$, $\mathfrak{d}'$ aus $\mathfrak{m}$, $\mathfrak{a}$, $\mathfrak{d}$ hervor, $\mathfrak{a}' = (\mathfrak{m}', \mathfrak{d}')$. Da nun in den Basiselementen von $\mathfrak{d}$ nur $x_{\varrho+1} \dots x_n$ vorkommen, die nur identisch transformiert werden, so sind $\mathfrak{d}$ und $\mathfrak{d}'$ isomorph. Wegen der Transformiertheit von $\mathfrak{m}$ folgt, wie im Zusatz zu Hilfssatz 1 bewiesen wurde, dasselbe für $\mathfrak{m}$ und $\mathfrak{m}'$. Da ferner die Isomorphie beide Mal durch Vertauschen der x mit den x' und der Elemente von U mit denen von $U \cdot U'$ besteht, so sind auch $\mathfrak{a}$ und $\mathfrak{a}'$ isomorph. Da der Satz für $\mathfrak{a}'$ bereits bewiesen ist, gilt er also auch für $\mathfrak{a}$, q. e. d.

Hilfssatz 3. Voraussetzung. *Es sei*

$$\mathfrak{m} = (f_1(x_1 \dots x_n y) \dots f_t(x_1 \dots x_n y))$$

ein Ideal in $\mathsf{P}(y)[x_1 \dots x_n]$, *dabei sei* y *transzendent in bezug auf* $\mathsf{P}[x_1 \dots x_n]$. $\mathfrak{m}_\xi = (f_1(x_1 \dots x_n \xi) \dots f_t(x_1 \dots x_n \xi))$ *sei das Ideal in* $\mathsf{P}[x_1 \dots x_n]$, *das aus* $\mathfrak{m}$ *durch Vertauschen von* y *mit einem Element* ξ *aus* P *hervorgeht. Es sei* $k(x_1 \dots x_n y) \not\equiv 0(\mathfrak{m})$. Ohne Beschränkung der Allgemeinheit können die Polynome f_i $[i = 1 \dots t]$ und k als ganz in y angenommen werden, so daß für jedes ξ aus P die Polynome $f_i(x_1 \dots x_n \xi)$ und $k(x_1 \dots x_n \xi)$ definiert sind.

Behauptung. *Es gibt ein* ξ *in* P, *so daß*

$$k(x_1 \dots x_n \xi) \not\equiv 0(\mathfrak{m}_\xi)$$

ist.

Beweis. 1. Zusammenhang zwischen Teilbarkeits- und Rangfragen. Es sei

$$g(x_1 \dots x_n y) \equiv 0(\mathfrak{m}).$$

Nach Satz 3 gibt es eine Darstellung

$$g(x_1 \dots x_n y)$$
$$= \varphi_1(x_1 \dots x_n y) f_1(x_1 \dots x_n y) + \dots + \varphi_t(x_1 \dots x_n y) f_t(x_1 \dots x_n y),$$

so daß $[\varphi_i] \leqq [g] + 2m(t, q, n)$ ist. Dabei ist wieder q der Maximalgrad der $f_i(x_1 \dots x_n y)$ in $x_1 \dots x_n$.

z_σ $[\sigma = 1 \dots s]$ seien die verschiedenen Potenzprodukte von $x_1 \dots x_n$, für die $[z_\sigma] \leqq [g] + q + 2m(t, q, n)$ ist. ζ_ϱ $[\varrho = 1 \dots r]$ seien die verschiedenen Potenzprodukte von $x_1 \dots x_n$, für die $[\zeta_\varrho] \leqq [g] + 2m(t, q, n)$ ist.

Wegen der Gradbeschränkung der einzelnen Terme in der Darstellung von g kann man diese Darstellung auf die Form bringen:

$$G(z_1 \dots z_s y) = \bar{\varphi}_1(y) F_1(z_1 \dots z_s y) + \dots + \bar{\varphi}_{t \cdot r}(y) F_{t \cdot r}(z_1 \dots z_s y).$$

Dabei ist $G(z_1 \dots z_s y) = g(x_1 \dots x_n y)$; die $F_i(z_1 \dots z_s y)$ haben die Gestalt $\zeta_\varrho \cdot f_k(x_1 \dots x_n y)$ und es sind die F_i und G linear in $z_1 \dots z_s$. Da nun G linear von den F_i abhängt, so haben die Matrizes

$$A = \left\| \begin{matrix} g_1(y) f_{11}(y) \cdots f_{1,t \cdot r}(y) \\ \cdots\cdots\cdots\cdots \\ g_s(y) f_{s1}(y) \cdots f_{s,t \cdot r}(y) \end{matrix} \right\| \quad \text{und} \quad B = \left\| \begin{matrix} f_{11}(y) \cdots f_{1,t \cdot r}(y) \\ \cdots\cdots\cdots \\ f_{s1}(y) \cdots f_{s,t \cdot r}(y) \end{matrix} \right\|$$

denselben Rang. Dabei bedeuten g_i und f_{ij} die Koeffizienten von z_i in G bzw. F_j.

Haben andererseits diese beiden Matrizes denselben Rang, so ist G linear abhängig von den F_i; ersetzt man in G und F_i wieder die z_σ durch die Potenzprodukte von $x_1 \dots x_n$, so ergibt sich daraus $g \equiv 0 (\mathfrak{m})$. Die beiden Matrizes haben also dann und nur dann denselben Rang, wenn g durch $\mathfrak{m}$ teilbar ist. Dieselben Überlegungen gelten, wenn für y ein Element ξ aus P gesetzt wird. An Stelle der $\varphi_i(x_1 \dots x_n y)$ treten dann Polynome $\varphi_{\xi i}(x_1 \dots x_n)$, die in $x_1 \dots x_n$ denselben Gradbeschränkungen genügen. Es gilt also auch hier: $g(x_1 \dots x_n \xi)$ ist dann und nur dann durch $\mathfrak{m}_\xi$ teilbar, wenn die beiden Matrizes, die aus A und B durch die Substitution $y = \xi$ hervorgehen, denselben Rang haben.

2. Wegen $k(x_1 \dots x_n y) \not\equiv 0 (\mathfrak{m})$ haben die Matrizes A' und B', die analog den Matrizes A und B aus $k(x_1 \dots x_n y)$ gebildet sind, verschiedenen Rang. In A' gibt es also eine nicht verschwindende Determinante, deren Rang um 1 höher ist als der von B'. Da nun P unendlich viele Elemente enthält, so kann y in P so zu ξ spezialisiert werden, daß diese Determinante von 0 verschieden bleibt. Ersetzt man y in A' und B' durch dies ξ, so behalten sie also verschiedenen Rang. Es wird also

$$k(x_1 \dots x_n \xi) \not\equiv 0 (\mathfrak{m}_\xi)$$

q. e. d.

Mit den Hilfssätzen 2 und 3 läßt sich jetzt der Hentzeltsche Nullstellensatz beweisen.

Definition 1. Unter einem *vollständigen Nullstellensystem* eines Ideals $\mathfrak{m}$ ist ein System von je einer Nullstelle von jedem zu $\mathfrak{m}$ gehörigen Primideal zu verstehen, je vom Transzendenzgrad dieses Primideals.

Definition 2. Es sei $\xi_1^{(i)} \dots \xi_n^{(i)}$ $[i = 1 \dots m]$ ein vollständiges Nullstellensytem von $\mathfrak{m}$, dann heißt $\mathfrak{o}_i = (x_1 - \xi_1^{(i)}, \dots, x_n - \xi_n^{(i)})$ ein zu $\mathfrak{m}$ gehöriges *Nullstellenideal.*

Aus der Definition folgt: $\mathfrak{o}_i$ ist Primideal in

$$\mathfrak{R}_i = \mathfrak{R}(\xi_1^{(i)} \dots \xi_n^{(i)}) = \mathsf{P}(\xi_1^{(i)} \dots \xi_n^{(i)})\,[x_1 \dots x_n].$$

Satz 5 [der Hentzeltsche Nullstellensatz]. Voraussetzung. $\xi_1^{(i)} \dots \xi_n^{(i)}$ $[i = 1 \dots m]$ *sei ein vollständiges Nullstellensystem des Ideals* $\mathfrak{m} = (f_1 \dots f_t)$. $\mathfrak{o}_i$ $[i = 1 \dots m]$ *seien die zugehörigen Nullstellenideale.* q *sei der Maximalgrad der* $f_1 \dots f_t$. *Es sei*

$$\varkappa(t, q, n) = q + \prod_{\lambda=1}^{n} \left[(q \cdot t)^{2^{\lambda-1} \cdot \prod_{i=1}^{n-\lambda} (2^{n-i+1})} - 1 \right] = q + v(t, q, n).$$

Behauptung. *Aus*

$$g \equiv 0\,(\mathfrak{m}, \mathfrak{o}_i^{\varkappa}) \quad \textit{in} \quad \mathfrak{R}_i = \mathfrak{R}(\xi_1^i \dots \xi_n^i) \quad \textit{für} \quad i = 1 \dots m$$

folgt stets

$$g \equiv 0\,(\mathfrak{m}).$$

Hentzelt spricht den Satz nur für algebraische Nullstellen aus in der folgenden zweiten Fassung:

Satz 5a. Voraussetzung. $\xi_1 \dots \xi_n$ *sei ein beliebiges Wertsystem aus dem zu* P *gehörenden algebraisch abgeschlossenen Körper. Es sei*

$$\mathfrak{a} = (x_1 - \xi_1, \dots, x_n - \xi_n).$$

Behauptung. *Aus*

$$g \equiv 0\,(\mathfrak{m}, \mathfrak{a}^{\varkappa})$$

für jedes solche Wertsystem folgt stets

$$g \equiv 0\,(\mathfrak{m}).$$

Ist $\xi_1 \dots \xi_n$ nicht algebraische Nullstelle von $\mathfrak{m}$, so ist $(\mathfrak{m}, \mathfrak{a}^{\varkappa}) = \mathfrak{o}$, also sicher $g \equiv 0\,(\mathfrak{m}, \mathfrak{a}^{\varkappa})$. Statt der Bedingung „für jedes beliebige Wertsystem" kann man also auch setzen „für jede algebraische Nullstelle von $\mathfrak{m}$".

Beweis. Der Satz soll für beide Fassungen bewiesen werden. Zum Beweis sind zunächst einige Vorbemerkungen nötig.

1. Ohne Beschränkung der Allgemeinheit darf angenommen werden, daß der zugrunde gelegte Körper $\bar{\mathsf{P}}$ unendlich viele Elemente enthält. Der Satz sei nämlich in diesem Fall bewiesen. $\mathfrak{m}$ sei definiert in $\mathfrak{R} = \mathsf{P}[x_1 \dots x_n] = \bar{\mathsf{P}}(u_{11} \dots u_{nn})\,[x_1 \dots x_n]$, wo $\bar{\mathsf{P}}$ nur endlich viele Elemente enthält. Es sei $\bar{\mathsf{P}}' = \bar{\mathsf{P}}(s)$, wo s transzendent in bezug auf $\bar{\mathsf{P}}$ sei. $\mathfrak{m}'$ sei definiert in $\mathfrak{R}' = \mathsf{P}'[x_1 \dots x_n] = \bar{\mathsf{P}}'(u_{11} \dots u_{nn})\,[x_1 \dots x_n]$

und habe dieselbe Basis wie $\mathfrak{m}$. Die Nullstellen von $\mathfrak{m}$ und $\mathfrak{m}'$ stimmen dann miteinander überein. Ein Polynom g in $\mathfrak{R}$, das die Voraussetzung der Sätze 5 und 5a für $\mathfrak{m}$ erfüllt, erfüllt sie also auch für $\mathfrak{m}'$. Nach Voraussetzung ist also

$$g \equiv 0 (\mathfrak{m}').$$

Es gibt also ein Polynom $k(s)$ in $\mathsf{P}(s)$, als dessen niedrigster Koeffizient die Einheit E aus P angenommen werden kann, so daß

$$k(s) \cdot g = g_1 f_1 + \ldots + g_t f_t$$

wird, wobei die g_i ganz in s sind. Durch Vergleich der Koeffizienten der niedrigsten in k auftretenden Potenz von s erhält man daraus

$$g = g_1' f_1 + \ldots + g_t' f_t$$

mit $g_i' \equiv 0 (\mathfrak{R})$, D. h. aber $g \equiv 0 (\mathfrak{m})$.

2. Es ist stets

$$\varkappa(t, q, n) \geqq \varkappa(t, q, n-1).$$

Ist nämlich $t = q = 1$, so wird

$$v(1, 1, n) = v(1, 1, n-1) = 0,$$

also

$$\varkappa(1, 1, n) = \varkappa(1, 1, n-1) = 1.$$

Es sei $q \cdot t \geqq 2$. Spaltet man von $v(t, q, n)$ den letzten Faktor ab, so erhält man die Gleichung

$$\begin{aligned} v(t, q, n) &= \prod_{\lambda=1}^{n-1} \left[(q \cdot t)^{2^{\lambda-1} \prod_{i=1}^{n-\lambda} (2^{n-i}+1)} - 1 \right] \cdot [(q \cdot t)^{2^{n-1}} - 1] \\ &= v_1(t, q, n) \cdot [(q \cdot t)^{2^{n-1}} - 1] \geqq v_1(t, q, n) \end{aligned}$$

wegen $q \cdot t \geqq 2$. Wegen

$$\prod_{i=1}^{n-\lambda} (2^{n-i}+1) \geqq \prod_{i=1}^{n-\lambda-1} (2^{n-i-1}+1)$$

gilt ferner

$$v_1(t, q, n) \geqq v(t, q, n-1)$$

und somit

$$v(t, q, n) \geqq v(t, q, n-1),$$

also auch

$$\varkappa(t, q, n) \geqq \varkappa(t, q, n-1).$$

3. Es sei $l \geqq \prod_{\lambda=1}^{n} (l_\lambda - 1)$, dann wird

$$\mathfrak{a}^l \equiv 0 ((x_1 - \xi_1)^{l_1} \ldots (x_n - \xi_n)^{l_n}).$$

Es ist nämlich

$$\mathfrak{a}^l = ((x - \xi_1)^l, \ldots, \prod_{\lambda=1}^{n} (x_\lambda - \xi_\lambda)^{\varepsilon_\lambda} [\sum_{\lambda=1}^{n} \varepsilon_\lambda = l], \ldots, (x_n - \xi_n)^l).$$

Und es wird allgemein für $\sum_{\lambda=1}^{n} \varepsilon_\lambda = l$

$$\prod_{\lambda=1}^{n} (x_\lambda - \xi_\lambda)^{\varepsilon_\lambda} \equiv 0\,((x_1 - \xi_1)^{l_1} \dots (x_n - \xi_n)^{l_n}).$$

Für den Beweis sollen ferner einige Bezeichnungen definiert werden.

4. $E_n(x_n)$ sei der Elementarteiler n-ter Stufe von $\mathfrak{m}$ [N. § 1, 6], l_n sei eine Zahl $\geqq [E_n(x_n)]$. Nach Zusatz 2 von Hilfssatz 1 kann man für transformierte Ideale, auf die sich der Beweis zunächst beschränken wird, setzen

$$l_n = (q \cdot t)^{(2^{n-1})}$$

Weiter sei

$$l_\lambda = N(t, q, \lambda, \prod_{i=\lambda+1}^{n} l_i) = (t \cdot q \cdot \prod_{i=\lambda+1}^{n} l_i)^{(2^{(\lambda-1)})}.$$

Es wird dann

$$\prod_{\lambda=1}^{n} (l_\lambda - 1) = v(t, q, n) < \varkappa(t, q, n).$$

Nach der dritten Vorbemerkung erlaubt diese Darstellung von v den Schluß: Aus

$$g \equiv 0\,(\mathfrak{m}, \mathfrak{a}^\varkappa)$$

folgt

$$g \equiv 0\,(\mathfrak{m}, (x_1 - \xi_1)^{l_1}; \dots (x_n - \xi_n)^{l_n}).$$

Zur Abkürzung sei gesetzt

$$\mathfrak{b}_i = ((x_i - \xi_i)^{l_i} \dots (x_n - \xi_n)^{l_n}) \quad \text{für} \quad i = 1, \dots, n.$$

Aus

$$g \equiv 0\,(\mathfrak{m}, \mathfrak{a}^\varkappa)$$

folgt also

$$g \equiv 0\,(\mathfrak{m}, \mathfrak{b}_1).$$

5. $\left.\begin{matrix} \xi_1^1 \dots \xi_n^1 \\ \dots\dots \\ \xi_1^p \dots \xi_n^p \end{matrix}\right\}$ seien die Nullstellen der zu $\mathfrak{m}$ gehörenden Primideale 0-ter Dimension. Die Wurzeln von $E_n(x_n)$ gehören der Reihe $\xi_n^1 \dots \xi_n^p$ an [N. § 1, 9].

Der Beweis des Satzes soll nun durch vollständige Induktion geführt werden.

1. $n = 1$. $\mathfrak{m} = (f(x))$ ist Hauptideal. Die beiden Formulierungen des Satzes besagen hier genau dasselbe, da alle Nullstellen vom Transzendenzgrad 0, also algebraisch sind. Es sei

$$f(x) = (x - \xi^1)^{\varepsilon_1} \dots (x - \xi^m)^{\varepsilon_m}.$$

$\xi^1 \dots \xi^m$ sind die einzigen Nullstellen von $\mathfrak{m}$. Es ist

$$\varkappa(1, q, 1) \geqq q \geqq \max_{i=1 \dots m} \varepsilon_i.$$

Es sei

$$g \equiv 0(\mathfrak{m}, (x-\xi^i)^\varkappa) \quad \text{für} \quad i = 1 \ldots m.$$

Dann ist

$$g = h_{i1} f + h_{i2}(x-\xi^i)^\varkappa \quad \text{für} \quad i = 1 \ldots m.$$

Also gilt

$$g \equiv 0\left(\prod_{i=1}^{m}(x-\xi^i)^{c_i}\right),$$

d. h.

$$g \equiv 0(\mathfrak{m}).$$

2. Angenommen, der Satz sei für $n = r-1$ bereits bewiesen. Es sei $n = r$. a) Angenommen, $\mathfrak{m}$ sei transformiert. Entsprechend den Voraussetzungen der zweiten Fassung des Satzes sei nun

$$g \equiv 0(\mathfrak{m}, \mathfrak{a}^\varkappa)$$

für jedes Wertsystem $\xi_1 \ldots \xi_r$. Durch die Spezialisierung $x_r = \xi_r$ gehe $\mathfrak{m}$ über in $\overline{\mathfrak{m}}$, g in $\bar{g}$, $\mathfrak{a}$ in $\bar{\mathfrak{a}} = (x_1 - \xi_1, \ldots, x_{r-1} - \xi_{r-1})$, und es wird

$$\bar{g} \equiv 0(\overline{\mathfrak{m}}, \bar{\mathfrak{a}}^\varkappa).$$

Diese Kongruenz gilt nach Voraussetzung für jedes ξ_r, das in P liegt, sie gilt also nach Hilfssatz 3 auch, wenn in ihr ξ_r durch ein in bezug auf P transzendentes Element, also z. B. durch x_r, ersetzt wird, das zu P adjungiert wird. Dann aber ist $\bar{g} = g$, und $\overline{\mathfrak{m}}$ geht aus $\mathfrak{m}$ durch Adjunktion von x_r zu P hervor. Die in bezug auf x_r ganzen Polynome von $\overline{\mathfrak{m}}$ bilden dann, wegen der Transformiertheit von $\mathfrak{m}$, das $r-1$-te Grundideal $\mathfrak{g}_{r-1}$ von $\mathfrak{m}$. Es ist also

$$g \equiv 0(\overline{\mathfrak{m}}; \bar{\mathfrak{a}}^{\varkappa(t,q,r)}).$$

Wegen $\varkappa(t,q,r) \geqq \varkappa(t,q,r-1)$ folgt daraus

$$g \equiv 0(\overline{\mathfrak{m}}, \bar{\mathfrak{a}}^{\varkappa(t,q,r-1)})$$

für jedes Wertesystem $\xi_1 \ldots \xi_{r-1}$. Da t die Anzahl der Basiselemente von $\overline{\mathfrak{m}}$, q eine obere Schranke für ihren Grad ist, so folgt nach Voraussetzung

$$g \equiv 0(\overline{\mathfrak{m}}).$$

Da g ganz ist in bezug auf x_r, ist also

$$g \equiv 0(\mathfrak{g}_{r-1}).$$

Dasselbe gilt unter der Voraussetzung der ersten Fassung dieses Satzes. Ihr entsprechend sei $g \equiv 0(\mathfrak{m}, \mathfrak{o}_i^\varkappa)$ für $i = 1 \ldots m$. Bei der Adjunktion von x_r zum Körper P gehen die Nullstellenideale $\mathfrak{o}_i$, die Nullstellen vom Transzendenzgrad 0 entsprechen, in das Einheitsideal $\mathfrak{o}$ über. Aus den anderen Nullstellenidealen, in denen ξ_r Parameter ist, der gleich x_r gesetzt werden kann, entstehen Ideale $\bar{\mathfrak{o}}_i$, die aus den $\mathfrak{o}_i$ durch Streichung des

letzten Basiselementes hervorgehen. Da die Nullstellen von $\mathfrak{g}_{r-1}$ aus denen von $\mathfrak{m}$ durch Streichung der Nullstellen vom Transzendenzgrad 0 hervorgehen, so sind diese $\bar{\mathfrak{o}}_i$ die dem Ideal $\overline{\mathfrak{m}}$ zugehörigen Nullstellenideale. Wie oben folgt also aus

$$g \equiv 0(\mathfrak{m}, \mathfrak{o}_i^{\varkappa}) \quad \text{für} \quad i = 1 \ldots m$$

stets

$$g \equiv 0(\mathfrak{g}_{r-1}).$$

Enthält $\mathfrak{m}$ *kein Primideal 0-ter Dimension*, so ist $\mathfrak{g}_{r-1} = \mathfrak{m}$, es wird also $g \equiv 0(\mathfrak{m})$, und der *Satz ist bewiesen.*

Es kann also angenommen werden, $\mathfrak{m}$ habe Primideale 0-ter Dimension mit den Nullstellen $\xi_1^j \ldots \xi_r^j$ $(j = 1 \ldots p)$. Für den weiteren Beweis der *zweiten Fassung* des Satzes genügt es, wenn an Stelle sämtlicher Wertsysteme nur die Systeme $\xi_1^{i_1} \ldots \xi_r^{i_r}$ betrachtet werden, dabei sind $i_1 \ldots i_r$ irgendwelche r gleiche oder verschiedene Zahlen der Reihe $1 \ldots p$.

Bisher hatte sich ergeben:

1. $g \equiv 0(\mathfrak{g}_{r-1})$; es ist also $E_r(x_r) \cdot g \equiv 0(\mathfrak{m})$, wobei die Wurzeln von $E_r(x_r)$ der Reihe $\xi_r^1 \ldots \xi_r^p$ angehören. Da $\mathfrak{m}$ transformiert ist, so gibt es aus Symmetriegründen Polynome $E_i(x_i)$ $[i = 1 \ldots r]$, so daß $E_i(x_i)\, g_{r-1} \equiv 0(\mathfrak{m})$, also auch $E_i \cdot g \equiv 0(\mathfrak{m})$ ist. Die Wurzeln von $E_i(x_i)$ gehören der Reihe $\xi_i^1 \ldots \xi_i^p$ an.

2. $g \equiv 0(\mathfrak{m}, \mathfrak{d}_1)$. Es soll gezeigt werden, daß hieraus bereits die Teilbarkeit von g durch $\mathfrak{m}$ folgt. Angenommen, es sei bereits gezeigt:

$$g \equiv 0(\mathfrak{m}, \mathfrak{d}_\nu),$$

d. h.

$$g \equiv 0(\mathfrak{m}, (x_\nu - \xi_\nu^{i_\nu})^{l_\nu}, \mathfrak{d}_{\nu+1}),$$

so wird

$$g \equiv h(x_1 \ldots x_r) \cdot (x_\nu - \xi_\nu^{i_\nu})^{l_\nu}(\mathfrak{m}, \mathfrak{d}_{\nu+1}).$$

Nach 1. gilt

$$E_\nu(x_\nu) \cdot g \equiv 0(\mathfrak{m}).$$

Also wird

$$E_\nu \cdot h \cdot (x_\nu - \xi_\nu^{i_\nu})^{l_\nu} \equiv 0(\mathfrak{m}, \mathfrak{d}_{\nu+1}).$$

Nach dem Zusatz von Hilfssatz 2 gibt es also ein Polynom $K^{i_{\nu+1} \cdots i_r}(x_\nu)$, so daß

$$K^{i_{\nu+1} \cdots i_r}(x_\nu)\, h \equiv 0(\mathfrak{m}, \mathfrak{d}_{\nu+1})$$

und

$$[K^{i_{\nu+1} \cdots i_r}(x_\nu)] \leqq N(t, q, \nu, \prod_{i=\nu+1}^{r} l_i) = l_\nu.$$

$(x_\nu - \xi_\nu^{i_\nu})^{l_\nu} \cdot E_\nu(x_\nu)$ und $K^{i_{\nu+1} \cdots i_r}(x_\nu)$ haben also beide die Eigenschaft, daß ihr Produkt mit h durch $(\mathfrak{m}, \mathfrak{d}_{\nu+1})$ teilbar ist. Damit gilt dasselbe

für ihren größten gemeinsamen Teiler, dessen Wurzeln sicher alle auch Wurzeln dieser beiden Polynome sind, und der nicht von höherem Grad ist als sie. Es ist also für

$$E^{i_\nu i_{\nu+1}\cdots i_r}(x_\nu) = (K^{i_{\nu+1}\cdots i_r}(x_\nu);\ E_\nu(x_\nu)\cdot(x_\nu - \xi_\nu^{i_\nu})^{l_\nu})$$

1. $E^{i_\nu\cdots i_r}(x_\nu)\cdot h(x_1\ldots x_r) \equiv 0\,(\mathfrak{m},\ \mathfrak{d}_{\nu+1})$;

2. $[E^{i_\nu\cdots i_r}(x_\nu)] \leqq l_\nu$, da dasselbe für $K^{i_{\nu+1}\cdots i_r}(x_\nu)$ gilt.

3. Die Wurzeln von $E^{i_\nu\cdots i_r}(x_\nu)$ gehören der Reihe $\xi_\nu^1\ldots\xi_\nu^p$ an, da dasselbe für $E_\nu(x_\nu)\cdot(x_\nu - \xi_\nu^{i_\nu})^{l_\nu}$ gilt.

Es sei

$$E^{i_\nu\cdots i_r}(x_\nu) = (x_\nu - \xi_\nu^{i_\nu})^{d_{i_\nu}\cdots i_r}\cdot D^{i_\nu\cdots i_r}(x_\nu),$$

dabei sei $\xi_\nu^{i_\nu}$ nicht mehr Wurzel von $D^{i_\nu\cdots i_r}(x_\nu)$. Es wird

$$d_{i_\nu\ldots i_r} \leqq l_\nu.$$

Da sämtliche Polynome $E^{1i_{\nu+1}\cdots i_r}(x_\nu)\ldots E^{pi_{\nu+1}\cdots i_r}(x_\nu)$ nur Wurzeln aus der Reihe $\xi_\nu^1\ldots\xi_\nu^p$ haben, so sind die Polynome $D^{1i_{\nu+1}\cdots i_r}(x_\nu)\ldots D^{pi_{\nu+1}\cdots i_r}(x_\nu)$ teilerfremd. Es wird also

$$\mathfrak{d} = (D^{1i_{\nu+1}\cdots i_r}(x_\nu)\ldots D^{pi_{\nu+1}\cdots i_r}(x_\nu)) = \mathfrak{o}.$$

Nun ist

$$\begin{aligned} D^{i_\nu\cdots i_r}(x_\nu)\,g &\equiv (x_\nu - \xi_\nu^{i_\nu})^{l_\nu}\cdot h(x_1\ldots x_r)\,D^{i_\nu\cdots i_r}(x_\nu) \\ &= (x_\nu - \xi_\nu^{i_\nu})^{l_\nu - d_{i_1}\ldots i_r}E^{i_\nu\cdots i_r}(x_\nu)\cdot h(x_1\ldots x_r) \equiv 0\,(\mathfrak{m},\ \mathfrak{d}_{\nu+1}). \end{aligned}$$

Das gilt für $i_\nu = 1\ldots p$, also ist

$$\mathfrak{d}\cdot g \equiv 0\,(\mathfrak{m},\ \mathfrak{d}_{\nu+1}).$$

Da nun $\mathfrak{d} = \mathfrak{o}$ das Einheitselement enthält, so wird

$$g \equiv 0\,(\mathfrak{m},\ \mathfrak{d}_{\nu+1}).$$

Setzt man für ν nacheinander die Werte $1\ldots r$, so erhält man

$$g \equiv 0\,(\mathfrak{m}).$$

Damit ist der *Satz* in seiner *zweiten Fassung* für transformierte Ideale *bewiesen*. Zum völligen Beweis der ersten Fassung genügt der Nachweis, daß aus

$$g \equiv 0\,(\mathfrak{m},\ \mathfrak{o}^\varkappa)$$

für jedes Nullstellenideal von $\mathfrak{m}$ stets folgt

$$g \equiv 0\,(\mathfrak{m},\ \mathfrak{a}^\varkappa)$$

für jedes

$$\mathfrak{a} = (x_1 - \xi_1, \ldots, x_r - \xi_r).$$

Es sei also

$$g \equiv 0\,(\mathfrak{m}, \mathfrak{o}_i^{\varkappa})$$

für jedes Nullstellenideal von $\mathfrak{m}$; $\xi_1 \ldots \xi_r$ sei ein beliebiges Wertesystem

$$\mathfrak{a} = (x_1 - \xi_1; \ldots; x_r - \xi_r).$$

Es soll gezeigt werden: $g \equiv 0\,(\mathfrak{m}, \mathfrak{a}^{\varkappa})$. Dabei sind drei Fälle zu unterscheiden:

1. $\xi_1 \ldots \xi_r$ ist keine algebraische Nullstelle von $\mathfrak{m}$. Dann ist $(\mathfrak{m}, \mathfrak{a}^{\varkappa}) = \mathfrak{o}$, also ist sicher

$$g \equiv 0\,(\mathfrak{m}, \mathfrak{a}^{\varkappa}).$$

2. $\xi_1 \ldots \xi_r$ ist Nullstelle von einem der zu $\mathfrak{m}$ gehörigen Primideale 0-ter Dimension, dann gehört $\mathfrak{a}$ zu den Nullstellenidealen, also ist auch

$$g \equiv 0\,(\mathfrak{m}, \mathfrak{a}^{\varkappa}).$$

3. $\xi_1 \ldots \xi_r$ ist algebraische Nullstelle von $\mathfrak{m}$, aber nicht Nullstelle von einem der zu $\mathfrak{m}$ gehörenden Primideale 0-ter Dimension.

Nun ist $(\mathfrak{m}, \mathfrak{a}^{\varkappa})$ ein Primärideal 0-ter Dimension, denn es ist $(\mathfrak{m}, \mathfrak{a}^{\varkappa}) \equiv 0\,(\mathfrak{a})$ wegen $\mathfrak{m} \equiv 0\,(\mathfrak{a})$; andererseits ist $\mathfrak{a}^{\varkappa} \equiv 0\,(\mathfrak{m}, \mathfrak{a}^{\varkappa})$. Also sind alle zu $(\mathfrak{m}, \mathfrak{a}^{\varkappa})$ gehörenden Primideale Teiler des Primideals $\mathfrak{a}$, und dieses ist selbst ein zu $(\mathfrak{m}, \mathfrak{a}^{\varkappa})$ gehörendes Primideal. Als Primideal 0-ter Dimension hat aber $\mathfrak{a}$ außer $\mathfrak{o}$ keinen echten Teiler, ist also das einzige zu $(\mathfrak{m}, \mathfrak{a}^{\varkappa})$ gehörende Primideal. $(\mathfrak{m}, \mathfrak{a}^{\varkappa})$ ist also Primärideal und gehört zu $\mathfrak{a}$.

Es sei nun $\mathfrak{k}$ das kleinste gemeinsame Vielfache der in einer Zerlegung von $\mathfrak{m}$ auftretenden Primärideale 0-ter Dimension. Es wird also

$$\mathfrak{m} = [\mathfrak{g}_{r-1}; \mathfrak{k}].$$

Nach Voraussetzung ist

$$\mathfrak{k} \not\equiv 0\,(\mathfrak{a}).$$

Da $\mathfrak{a}$ Primideal ist, gilt also auch

$$\mathfrak{k}^{\lambda} \not\equiv 0\,(\mathfrak{a})$$

für jedes λ. Wegen $(\mathfrak{m}, \mathfrak{a}^{\varkappa}) \equiv 0\,(\mathfrak{a})$ folgt

$$\mathfrak{k}^{\lambda} \not\equiv 0\,(\mathfrak{m}, \mathfrak{a}^{\varkappa})$$

für jedes λ. Andererseits ist

$$\mathfrak{m} = [\mathfrak{g}_{r-1}; \mathfrak{k}] \equiv 0\,(\mathfrak{m}, \mathfrak{a}^{\varkappa}),$$

also gilt auch

$$\mathfrak{g}_{r-1} \cdot \mathfrak{k} \equiv 0\,(\mathfrak{m}, \mathfrak{a}^{\varkappa}).$$

Da $(\mathfrak{m}, \mathfrak{a}^{\varkappa})$ Primärideal ist, folgt

$$\mathfrak{g}_{r-1} \equiv 0\,(\mathfrak{m}, \mathfrak{a}^{\varkappa}).$$

Nun folgt aber, wie im Induktionsschluß bereits bewiesen ist, aus der Voraussetzung $g \equiv 0\,(\mathfrak{m}, \mathfrak{o}_i^{\varkappa})$ für jedes Nullstellenideal und der Annahme, daß der Satz für $r-1$ Variable bereits bewiesen ist,

$$g \equiv 0\,(\mathfrak{g}_{r-1}).$$

Es wird also

$$g \equiv 0\,(\mathfrak{m}, \mathfrak{a}^{\varkappa})$$

für jedes $\mathfrak{a}$. Da der Satz in der zweiten Fassung schon bewiesen ist, folgt

$$g \equiv 0\,(\mathfrak{m}).$$

Somit ist für transformierte Ideale der Satz auch in der *ersten Fassung bewiesen.*

b) $\mathfrak{m}$ sei nicht transformiert. Der Satz gilt für das zu $\mathfrak{m}$ gehörige transformierte Ideal $\mathfrak{m}'$. Die transzendenten Nullstellen von $\mathfrak{m}$ gehen durch die Transformation in die von $\mathfrak{m}'$ über. Die Nullstellenideale $\mathfrak{o}_i$ gehen also über in die Nullstellenideale $\mathfrak{o}_i'$ von $\mathfrak{m}'$. Das Polynom g gehe über in g'. Es sei

$$g \equiv 0\,(\mathfrak{m}, \mathfrak{o}_i^{\varkappa}) \qquad \text{für } i = 1 \ldots m.$$

Folglich ist

$$g' \equiv 0\,(\mathfrak{m}'; \mathfrak{o}_i'^{\varkappa}) \qquad \text{für } i = 1 \ldots m.$$

Also ist

$$g' \equiv 0\,(\mathfrak{m}').$$

Da g' transformiert ist, kann zurücktransformiert werden:

$$g \equiv 0\,(\mathfrak{m}).$$

Dasselbe gilt, wenn für die $\mathfrak{o}_i$ die Ideale $\mathfrak{a}$ der zweiten Fassung betrachtet werden, denn auch die algebraischen Nullstellen des nicht transformierten und des transformierten Ideals gehen durch die Transformation ineinander über. Der Satz ist damit in beiden Fassungen vollständig bewiesen.

§ 6.

Grundideale.

In den nächsten Paragraphen sollen nun die für ein Ideal charakteristischen Ideale und Polynome berechnet werden. Zunächst handelt es sich um die Bildung der Grundideale sowie der Norm und der Elementarteilerform. Dabei wird es nötig sein, zu dem in N. § 1, 5 definierten Modul $\mathfrak{M}_{\varrho-1}^{*}$ überzugehen, der die in bezug auf $x_1 \ldots x_{\varrho-1}$ einen festen Grad $n_{\varrho-1}$ nicht überschreitenden Polynome aus $\mathfrak{m}$ und nur diese enthält, aufgefaßt als Linearformen in den Potenzprodukten von $x_1 \ldots x_{\varrho-1}$. Die Berechnung der Zahl $n_{\varrho-1}$ wird in Satz 6 gegeben.

Satz 6. Voraussetzung. $\mathfrak{m}$ *sei ein transformiertes Ideal in* $\overline{\mathsf{P}}(u_{11} \dots u_{nn})[x_1 \dots x_n] = \mathsf{P}[x_1 \dots x_n]$, q *der Maximalgrad der gegebenen Basis von* $\mathfrak{m}$.

Behauptung. *Für das Restklassensystem* $\mathfrak{g}_\varrho \,|\, \mathfrak{m}$ *gibt es Repräsentanten der Restklassen, die in den Potenzprodukten von* $x_1 \dots x_\varrho$ *einen festen Grad* n_ϱ *nicht überschreiten. Dabei ist* n_ϱ *durch die Rekursionsformel gegeben*:

$$n_0 = 0; \quad n_\varrho = n_{\varrho-1} + \left[\sum_{i=0}^{n-1} q^{2i}\right] \cdot \left[1 + \binom{n_{\varrho-1}+\varrho-1}{\varrho-1}\right].$$

Beweis durch vollständige Induktion.

1. $\varrho = 0$. Der Satz legt den Repräsentanten des Restklassensystems überhaupt keine Beschränkung auf, ist also evident.

2. Angenommen, der Satz sei für $\varrho = 0 \dots \lambda - 1$ bereits bewiesen. Es sei $\varrho = \lambda$.

a) Angenommen, $\overline{\mathsf{P}}$ enthalte unendlich viele Elemente.

$$\mathfrak{m} = (f_{\lambda-1,1} \cdots f_{\lambda-1,t_{\lambda-1}})$$

sei die nach Satz 4 existierende und berechenbare ausgezeichnete $\lambda - 1$-te Idealbasis von $\mathfrak{m}$, deren Basiselemente nach Satz 4 den Grad $\bar{q} = \sum_{i=0}^{n-1} q^{2i}$ nicht überschreiten. Zur Abkürzung soll für den folgenden Beweis der Index $\lambda - 1$ in dieser Basis weggelassen werden. Wir schreiben also

$$\mathfrak{m} = (f_1 \cdots f_{t_{\lambda-1}}).$$

z_σ $[\sigma = 1 \dots s]$ seien die Potenzprodukte von $x_1 \dots x_{\lambda-1}$, die den Grad $n_{\lambda-1}$ nicht überschreiten. Es ist also $s = \binom{n_{\lambda-1}+\lambda-1}{\lambda-1}$. $\zeta_{\mu_\varkappa}$ $[\mu_\varkappa = 1 \dots m_\varkappa]$ seien die Potenzprodukte von $x_1 \dots x_{\lambda-1}$, die den Grad $n_{\lambda-1} - [f]_{\lambda-1}$ nicht überschreiten. Es ist also $m_\varkappa \leqq s$.

Es sei $\mathfrak{M}^*_{\lambda-1} = (f_1 \dots f_{t_{\lambda-1}};\ \zeta_1 f_1 \dots \zeta_{m_{t_{\lambda-1}}} f_{t_{\lambda-1}}) = (l_1 \dots l_{\bar{t}})$. Dann ist $\bar{t} < t_{\lambda-1} s$, und $\mathfrak{M}^*_{\lambda-1}$ kann aufgefaßt werden als Linearformenmodul in den z_σ mit Koeffizienten aus $\mathsf{P}[x_\lambda \dots x_n]$. Er enthält, da er aus der in Satz 4 definierten ausgezeichneten Idealbasis gebildet ist, alle und nur die Elemente aus $\mathfrak{m}$, die in $x_1 \dots x_{\lambda-1}$ den Grad $n_{\lambda-1}$ nicht übersteigen.

Auf den Modul $\mathfrak{M}^*_{\lambda-1}$ sollen die Methoden des Satzes 3 angewendet werden, dafür muß die Existenz einer regulären Determinante vom Range des Moduls nachgewiesen sein. Da $\overline{\mathsf{P}}$ unendlich viele Elemente enthält, läßt sich durch eine Transformation $x = V(y)$

$$\begin{aligned}
x_1 &= y_1 \\
&\cdots\cdots \\
x_{\lambda-1} &= y_{\lambda-1} \\
x_\lambda &= v_{\lambda\lambda} y_\lambda + \cdots + v_{\lambda n} y_n \\
&\cdots\cdots\cdots\cdots \\
x_n &= v_{n\lambda} y_\lambda + \cdots + v_{nn} y_n
\end{aligned}$$

stets erreichen, daß $\mathfrak{M}^*_{\lambda-1}$ übergeht in einen Modul $\mathfrak{M}^{*'}_{\lambda-1}$, der eine in y_λ reguläre Determinante enthält. Dabei sollen die v_{ij} Größen aus $\overline{\mathsf{P}}$ sein, und V soll eine nicht verschwindende Determinante haben. Da die Transformation die z_σ unverändert läßt, also an der Modulbildung nichts ändert, so entsteht $\mathfrak{M}^{*'}_{\lambda-1}$ auch, wenn man die Transformation $x = V(y)$ am Ideal $\mathfrak{m}$ vornimmt und dann in der angegebenen Weise den Modul bildet. $\mathfrak{m}$ ist transformiert, ist also aus einem Ideal $\overline{\mathfrak{m}}$ in $\overline{\mathsf{P}}[\bar{x}_1 \ldots \bar{x}_n]$ durch die Transformation $\bar{x} = U(x)$ und die Adjunktion der Elemente u_{ij} von U zum Körper $\overline{\mathsf{P}}$ entstanden. Durch $x = V(y)$ gehe $\mathfrak{m}$ in $\mathfrak{m}'$ über. Es wird nun $\bar{x} = UV(y) = W(y)$. Die Elemente w_{ij} der Matrix W sind dabei lineare Kombinationen der u_{ij} mit Koeffizienten aus $\overline{\mathsf{P}}$, da ferner V eine nicht verschwindende Determinante besitzt, so ist $U = WV^{-1}$; die Elemente von U lassen sich also auch umgekehrt durch die w_{ij} linear ausdrücken mit Koeffizienten aus $\overline{\mathsf{P}}$. Mit den u_{ij} sind also auch die w_{ij} Unbestimmte, und die Körper $\overline{\mathsf{P}}(u_{ij})$ und $\overline{\mathsf{P}}(w_{ij})$ sind identisch. Die Zuordnung $u_{ij} \sim w_{ij}$ und $x_k \sim y_k$ vermittelt also eine isomorphe Zuordnung zwischen $\mathfrak{m}$ und $\mathfrak{m}'$ sowie zwischen $\mathfrak{M}^*_{\lambda-1}$ und $\mathfrak{M}^{*'}_{\lambda-1}$, da diese beiden Moduln in durchaus entsprechender Weise aus den isomorphen Idealen gebildet sind. Da die Existenz der regulären Determinante für $\mathfrak{M}^{*'}_{\lambda-1}$ nachgewiesen ist, so gilt sie also auch für $\mathfrak{M}^*_{\lambda-1}$.

Es sei

$$\begin{aligned}
l_1 &= f_{11} z_1 + \cdots + f_{1s} z_s \\
&\cdots\cdots\cdots \\
l_{\bar{i}} &= f_{\bar{i}1} z_1 + \cdots + f_{\bar{i}s} z_s .
\end{aligned}$$

$p \leqq s$ sei der Rang von $\mathfrak{M}^*_{\lambda-1}$. In bezug auf $\mathfrak{M}^*_{\lambda-1}$ sollen die Polynome $D_{i_1 \ldots i_p}$, speziell $D_{1 \ldots p} = D$; F_{ij} und m_i genau wie in Satz 3 definiert werden. Das ist möglich, da $\mathfrak{M}^*_{\lambda-1}$ eine reguläre Determinante besitzt.

Es sei nun

$$k \equiv 0 (\mathfrak{g}_\lambda) .$$

Da $\mathfrak{m}$ transformiert ist, gibt es also nur ein von $x_{\lambda+1} \ldots x_n$ abhängendes Polynom $K^{(\lambda+1)} \neq 0$, so daß

$$K^{(\lambda+1)} k \equiv 0 (\mathfrak{m})$$

wird. Wegen $y_\lambda \equiv 0(\mathfrak{g}_{\lambda-1})$ ist ferner

$$k \equiv 0(\mathfrak{g}_{\lambda-1}).$$

Also gilt nach Voraussetzung

$$k \equiv g(\mathfrak{m}),$$

also auch

$$K^{(\lambda+1)} \cdot g \equiv 0(\mathfrak{m}),$$

wobei

$$[g]_{\lambda-1} \leqq n_{\lambda-1}$$

ist. Es ist also auch

$$[K^{(\lambda+1)} \cdot g]_{\lambda-1} \leqq n_{\lambda-1},$$

und somit gilt

$$K^{(\lambda+1)} \cdot g \equiv 0(\mathfrak{M}^*_{\lambda-1}).$$

Man setze wie in Satz 3

$$g = g_1^{(\lambda)} z_1 + \ldots + g_s^{(\lambda)} z_s$$

$$g_i^{(\lambda)} = G_i^{(\lambda)} + D \cdot j_i^{(\lambda)} \qquad \text{für} \quad i = 1 \ldots p,$$

so daß

$$[G_i^{(\lambda)}]_\lambda < [D]_\lambda = [D] \qquad \text{für} \quad i = 1 \ldots p$$

und

$$[j_i^{(\lambda)}] \leqq [g] \qquad \text{für} \quad i = 1 \ldots p$$

wird. Wie in Satz 3 wird dann

$$g = G + \sum_{i=1}^{p} m_i j_i^{(\lambda)},$$

$$G = G_1^{(\lambda)} z_1 + \ldots + G_p^{(\lambda)} z_p + G_{p+1}^{(\lambda)} z_{p+1} + \ldots + G_s^{(\lambda)} z_s.$$

Da $K^{(\lambda+1)}$ von x_λ unabhängig ist, so ergeben sich für $K^{(\lambda+1)} g$ die entsprechenden Zerlegungen durch Multiplikation von g, $g_i^{(\lambda)}$, $G_i^{(\lambda)}$ und $j_i^{(\lambda)}$ mit $K^{(\lambda+1)}$ in diesen Gleichungen und Ungleichungen; denn es bleibt

$$[K^{(\lambda+1)} G_i^{(\lambda)}]_\lambda < [D].$$

Wegen $g \equiv G(\mathfrak{M}^*_{\lambda-1})$ ist

$$K^{(\lambda+1)} G \equiv 0(\mathfrak{M}^*_{\lambda-1}),$$

d. h.

$$K^{(\lambda+1)} G = a_1 l_1 + \ldots + a_{\bar{\imath}} l_{\bar{\imath}},$$

$$K^{(\lambda+1)} G_i = a_1 f_{i1} + \ldots + a_{\bar{\imath}} f_{i\bar{\imath}}.$$

Wie in Satz 3 kann hierbei gesetzt werden

$$[a_i]_\lambda \leqq [D] \qquad \text{für } i = 1 \ldots p,$$

und wie dort zeigt man, daß daraus bereits folgt

$$[a_i]_\lambda \leqq \bar{q} \cdot p \quad [10] \qquad \text{für } i = 1 \ldots \bar{t},$$

d. h.

$$[a_i]_\lambda < \bar{q} \binom{n_{\lambda-1}+\lambda-1}{\lambda-1} \qquad \text{für } i = 1 \ldots \bar{t}.$$

Daraus folgt

$$[G_i]_\lambda \leqq \bar{q} + \bar{q} \binom{n_{\lambda-1}+\lambda-1}{\lambda-1} \qquad \text{für } i = 1 \ldots \bar{t},$$

$$[G]_\lambda \leqq n_{\lambda-1} + \bar{q}\left\{1 + \binom{n_{\lambda-1}+\lambda-1}{\lambda-1}\right\} = n_\lambda.$$

Da außerdem $k \equiv g(\mathfrak{m})$ und $g \equiv G(\mathfrak{m})$ ist, so ist auch

$$k \equiv G(\mathfrak{m}).$$

G ist also ein in bezug auf $x_1 \ldots x_\lambda$ beschränkter Repräsentant der Restklasse k aus $\mathfrak{g}_\lambda \,|\, \mathfrak{m}$.

b) $\bar{\mathsf{P}}$ enthalte nur endlich viele Elemente. s sei transzendent in bezug auf $\bar{\mathsf{P}}$. Dann enthält $\bar{\mathsf{P}}(s)$ sicher unendlich viele Elemente. $\mathfrak{m}'$ sei das Ideal in $\bar{\mathsf{P}}(u_{11} \ldots u_{nn}, s)[x_1 \ldots x_n]$, dessen Basis mit der von $\mathfrak{m}$ übereinstimmt. Nach a) gilt der Satz für $\mathfrak{m}'$. $\mathfrak{g}'_\varrho$, das ϱ-te Grundideal von $\mathfrak{m}'$, ist dann das durch Adjunktion von s aus $\mathfrak{g}_\varrho$, dem ϱ-ten Grundideal von $\mathfrak{m}$ hervorgehende Ideal [vgl. § 1, 4: Adjunktion von Unbestimmten zum Körper ändert nichts an der Eigenschaft eines Ideals, Grundideal eines anderen zu sein.]

Es sei $g \equiv 0\,(\mathfrak{g}_\varrho)$; dann ist auch $g \equiv 0\,(\mathfrak{g}'_\varrho)$, also gibt es ein $k'(s)$, so daß

$$g \equiv k'(\mathfrak{m}') \quad \text{und} \quad [k']_\varrho \leqq n_\varrho$$

ist. Es wird also

$$g = k' + c'_1 f_1 + \ldots + c'_t f_t.$$

Durch Multiplikation mit einem Polynom $\varkappa(s)$ aus $\bar{\mathsf{P}}(u_{11} \ldots u_{nn})[s]$ kann diese Gleichung in bezug auf s ganz gemacht werden. Dabei kann ohne Beschränkung der Allgemeinheit die Einheit E von $\bar{\mathsf{P}}$ als der niedrigste in $\varkappa(s)$ auftretende Koeffizient in $\varkappa(s)$ vorausgesetzt werden.

$$\varkappa \cdot g = k'' + c''_1 f_1 + \ldots + c''_t f_t.$$

Spaltet man diese Gleichung nach Potenzen von s auf und setzt die Koeffizienten der niedrigsten in $\varkappa(s)$ auftretenden Potenz gleich, so erhält man rechts und links

$$g = k + c_1 f_1 + \ldots + c_t f_t.$$

---

[10]) In Satz 3 steht an dieser Stelle statt p die Anzahl t der Basiselemente des Moduls. Benutzt wurde aber nur, daß diese Anzahl nicht kleiner als der Rang des Moduls ist. Der Rang p leistet also in dieser Ungleichung dasselbe.

Dabei sind die k; $c_1 \dots c_t$ die entsprechenden Koeffizienten von k''; $c_1'' \dots c_t''$. Es ist also

$$g \equiv k(\mathfrak{m}) \quad \text{und} \quad [k]_\varrho \leqq n_\varrho,$$

q. e. d.

Hilfssatz 4. Voraussetzung. *Es sei $\mathfrak{M}$ Modul aus Linearformen in $z_1 \dots z_s$ mit Koeffizienten aus $\mathsf{P}[x_\varrho \dots x_n]$. $\mathfrak{G}$ sei der zugehörige Grundmodul. $\mathfrak{M}'$ und $\mathfrak{G}'$ seien Moduln aus Linearformen in $z_1 \dots z_s$ mit Koeffizienten aus $\mathsf{P}[x_\varrho](x_{\varrho+1} \dots x_n)$, deren Basiselemente mit denen von $\mathfrak{M}$ bzw. $\mathfrak{G}$ übereinstimmen.*

Behauptung. *$\mathfrak{G}'$ ist Grundmodul von $\mathfrak{M}'$.*

Beweis. Es sei $c' \cdot g'(z) \equiv 0\,(\mathfrak{M}')$. Dabei sei $c' \neq 0$ eine Größe aus $\mathsf{P}[x_\varrho](x_{\varrho+1} \dots x_n)$ und $g'(z)$ eine Linearform in $z_1 \dots z_s$ mit Koeffizienten aus $\mathsf{P}[x_\varrho](x_{\varrho+1} \dots x_n)$. Dann gibt es ein Polynom $d^{(\varrho+1)} \neq 0$ aus $\mathsf{P}[x_{\varrho+1} \dots x_n]$, so daß

$$d^{(\varrho+1)} \cdot c' \cdot g'(z) \equiv 0\,(\mathfrak{M})$$

wird, und es ist

$$d^{(\varrho+1)} = e^{(\varrho+1)} \cdot f^{(\varrho+1)},$$

so daß

$$e^{(\varrho+1)} \cdot c' = c \quad \text{und} \quad f^{(\varrho+1)} \cdot g'(z) = g(z)$$

ganz sind in $x_{\varrho+1} \dots x_n$. Es ist also

$$c \cdot g(z) \equiv 0\,(\mathfrak{M}) \qquad c \neq 0$$

und somit

$$g(z) \equiv 0\,(\mathfrak{G}).$$

Es wird also auch

$$g'(z) = \frac{g(z)}{f^{(\varrho+1)}} \equiv 0\,(\mathfrak{G}').$$

Der Grundmodul von $\mathfrak{M}'$ ist also durch $\mathfrak{G}'$ teilbar. Ist andererseits

$$g'(z) \equiv 0\,(\mathfrak{G}'),$$

so gibt es ein Polynom $f^{(\varrho+1)} \neq 0$, so daß

$$f^{(\varrho+1)} \cdot g' = g \equiv 0\,(\mathfrak{G});$$

es gibt also ein c in $\mathsf{P}[x_\varrho \dots x_n]$, so daß

$$c \cdot g \equiv 0\,(\mathfrak{M})$$

und folglich auch

$$c \cdot g' \equiv 0\,(\mathfrak{M}')$$

wird. Also ist g' und somit auch $\mathfrak{G}'$ durch den Grundmodul von $\mathfrak{M}'$ teilbar. $\mathfrak{G}'$ ist also der Grundmodul von $\mathfrak{M}'$, q. e. d.

Folgerung aus Satz 6. $\mathfrak{g}_\varrho$ hat mod $\mathfrak{m}$ eine Basis, deren Elemente in $x_1 \dots x_\varrho$ den Grad n_ϱ nicht überschreiten. Da nun bereits die Basis-

elemente von $\mathfrak{m}$ in bezug auf $x_1 \dots x_\varrho$ den Grad q nicht überschreiten, und da für $\varrho > 0$ stets $n_\varrho \geqq q$ ist, so hat $\mathfrak{g}_\varrho$ für $\varrho > 0$ eine Basis, deren Elemente in $x_1 \dots x_\varrho$ den Grad n_ϱ nicht überschreiten.

Wie im Beweis von Satz 6 bemerkt wurde, besteht der Modul $\mathfrak{M}_\varrho^*$ aus der Gesamtheit der Elemente von $\mathfrak{m}$, die in $x_1 \dots x_\varrho$ den Grad n_ϱ nicht überschreiten. Entsprechend setzen wir nun fest:

Definition. 1. $\mathfrak{G}_\varrho^*$ sei der Modul aus Linearformen in den Potenzprodukten z_σ von $x_1 \dots x_\varrho$, der aus der Gesamtheit der Elemente aus $\mathfrak{g}_\varrho$ besteht, die in bezug auf $x_1 \dots x_\varrho$ den Grad n_ϱ nicht überschreiten. Nach der Folgerung aus Satz 6 enthält $\mathfrak{G}_\varrho^*$ dann eine Basis von $\mathfrak{g}_\varrho$.

2. $\mathfrak{M}_\varrho$ und $\mathfrak{G}_\varrho$ seien Moduln aus Linearformen in den Potenzprodukten z_σ von $x_1 \dots x_\varrho$, die aus der Gesamtheit der in $\mathfrak{m}$ bzw. in $\mathfrak{g}_\varrho$ enthaltenen Elementen bestehen. In $\mathfrak{M}_\varrho$ und $\mathfrak{G}_\varrho$ treten also unendlich viele z_σ auf, während jede einzelne Linearform nur endlich viele z_σ enthält.

Für das Folgende sei $\mathfrak{m}$ und somit auch $\mathfrak{g}_\varrho$ stets als transformiert vorausgesetzt [§ 1, 4]. Dann ist sicher $\mathfrak{G}_\varrho$ Grundmodul von $\mathfrak{M}_\varrho$. Für die Moduln $\mathfrak{M}_{\varrho-1}^*$; $\mathfrak{G}_{\varrho-1}^*$ $\mathfrak{M}_{\varrho-1}$ und $\mathfrak{G}_{\varrho-1}$ gilt.

Satz 7. 1. *$\mathfrak{G}_{\varrho-1}^*$ ist Grundmodul von $\mathfrak{M}_{\varrho-1}^*$.*

2. *Das Restklassensystem $\mathfrak{G}_{\varrho-1}^* | \mathfrak{M}_{\varrho-1}^*$ von $\mathfrak{G}_{\varrho-1}^*$ nach $\mathfrak{M}_{\varrho-1}^*$ ist isomorph demjenigen von $\mathfrak{G}_{\varrho-1}$ nach $\mathfrak{M}_{\varrho-1}$. In Zeichen*

$$\mathfrak{G}_{\varrho-1}^* | \mathfrak{M}_{\varrho-1}^* \sim \mathfrak{G}_{\varrho-1} | \mathfrak{M}_{\varrho-1}.$$

3. *$\mathfrak{M}_{\varrho-1}$ hat nur endlich viele von der Einheit E verschiedene Elementarteiler, nämlich die von $\mathfrak{M}_{\varrho-1}^*$.*

Beweis. 1. $\overline{\mathfrak{G}}_{\varrho-1}^*$ sei Grundmodul von $\mathfrak{M}_{\varrho-1}^*$. Es sei $g \equiv 0 (\mathfrak{G}_{\varrho-1}^*)$, dann ist $g \equiv 0 (\mathfrak{g}_{\varrho-1})$ und $[g]_{\varrho-1} \leqq n_{\varrho-1}$. Folglich gibt es ein Polynom $f^{(\varrho)} \neq 0$, so daß $f^{(\varrho)} \cdot g \equiv 0 (\mathfrak{m})$. Es ist $[f^{(\varrho)} \cdot g]_{\varrho-1} \leqq n_{\varrho-1}$, also ist $f^{(\varrho)} \cdot g \equiv 0 (\mathfrak{M}_{\varrho-1}^*)$ und somit $g \equiv 0 (\overline{\mathfrak{G}}_{\varrho-1}^*)$.

Ist andererseits $g \equiv 0 (\overline{\mathfrak{G}}_{\varrho-1}^*)$, dann existiert ein $f^{(\varrho)} \neq 0$, so daß $f^{(\varrho)} \cdot g \equiv 0 (\mathfrak{M}_{\varrho-1}^*)$. Es wird also $[f^{(\varrho)} \cdot g]_{\varrho-1} \leqq n_{\varrho-1}$, also auch $[g]_{\varrho-1} \leqq n_{\varrho-1}$. Außerdem ist $g \equiv 0 (\mathfrak{g}_{\varrho-1})$. Es ist also $g \equiv 0 (\mathfrak{G}_{\varrho-1}^*)$ und somit

$$\mathfrak{G}_{\varrho-1}^* = \overline{\mathfrak{G}}_{\varrho-1}^*, \quad \text{q. e. d.}$$

2. $\{g\}$ sei Restklasse aus $\mathfrak{G}_{\varrho-1} | \mathfrak{M}_{\varrho-1}$. Nach Satz 6 kann g so gewählt werden, daß $[g]_{\varrho-1} \leqq n_{\varrho-1}$ wird, also ist $g \equiv 0 (\mathfrak{G}_{\varrho-1}^*)$. Es wird also

$$\mathfrak{G}_{\varrho-1} | \mathfrak{M}_{\varrho-1} \sim \mathfrak{G}_{\varrho-1}^* | \mathfrak{M}_{\varrho-1}.$$

Es sei nun $\{g\}$ die Nullklasse aus $\mathfrak{G}_{\varrho-1}^* | \mathfrak{M}_{\varrho-1}$, d. h.

$$g \equiv 0 (\mathfrak{G}_{\varrho-1}^*) \quad \text{und} \quad g \equiv 0 (\mathfrak{M}_{\varrho-1}),$$

also ist

$$[g]_{\varrho-1} \leqq n_{\varrho-1} \qquad \text{und} \quad g \equiv 0 (\mathfrak{m}).$$

Daraus folgt

$$g \equiv 0\,(\mathfrak{M}^*_{\varrho-1}).$$

$\{g\}$ ist also auch Nullklasse aus $\mathfrak{G}^*_{\varrho-1}\,|\,\mathfrak{M}^*_{\varrho-1}$. Ist andererseits $\{g\}$ Nullklasse aus $\mathfrak{G}^*_{\varrho-1}\,|\,\mathfrak{M}^*_{\varrho-1}$, so ist wegen $\mathfrak{M}^*_{\varrho-1} \equiv 0\,(\mathfrak{M}_{\varrho-1})$ die Restklasse $\{g\}$ auch Nullklasse aus $\mathfrak{G}^*_{\varrho-1}\,|\,\mathfrak{M}^*_{\varrho-1}$. Es ist also

$$\mathfrak{G}^*_{\varrho-1}\,|\,\mathfrak{M}_{\varrho-1} \sim \mathfrak{G}^*_{\varrho-1}\,|\,\mathfrak{M}^*_{\varrho-1}.$$

Also auch

$$\mathfrak{G}_{\varrho-1}\,|\,\mathfrak{M}_{\varrho-1} \sim \mathfrak{G}^*_{\varrho-1}\,|\,\mathfrak{M}^*_{\varrho-1}, \quad \text{q. e. d.}$$

3. Für den Beweis der dritten Behauptung sei $x_{\varrho+1} \ldots x_n$ dem zugrunde gelegten Körper adjungiert. Nach Hilfssatz 4 bleibt dabei die Eigenschaft von $\mathfrak{G}^*_{\varrho-1}$ bzw. $\mathfrak{G}_{\varrho-1}$, Grundmodul von $\mathfrak{M}^*_{\varrho-1}$ bzw. $\mathfrak{M}_{\varrho-1}$ zu sein, erhalten. Der Koeffizientenbereich dieser Moduln ist also jetzt der Ring $\mathsf{P}\,[x_\varrho]\,(x_{\varrho+1} \ldots x_n)$, in dem jedes Ideal Hauptideal ist. Die Moduln können dann aufgefaßt werden als verallgemeinerte Abelsche Gruppen gegenüber der Addition, deren Multiplikatorenbereich der Koeffizientenring der Moduln ist. Der Satz über die bis auf Isomorphie eindeutige Darstellung einer Abelschen Gruppe endlicher Ordnung als direkte Summe endlich vieler größter zyklischer Gruppen, deren Ordnungen durcheinander teilbar sind, gilt auch hier, da für seinen Beweis nur vorausgesetzt werden muß, daß im Multiplikatorenring jedes Ideal Hauptideal ist. Als Ordnung einer Gruppe Γ ist jetzt definiert ein Element a des Multiplikatorenbereichs, derart daß $a \cdot \Gamma$ verschwindet, und daß a größter gemeinsamer Teiler aller Elemente dieser Eigenschaft ist.

Nun gibt es eine Darstellung

$$\mathfrak{M}^*_{\varrho-1} = (e_1\,\eta_1^{\mathfrak{f}}; \ldots e_r\,\eta_r); \qquad \mathfrak{G}^*_{\varrho-1} = (\eta_1; \ldots \eta_r),$$

$$\mathfrak{M}_{\varrho-1} = (e'_1\,\eta'_1; \ldots e'_{r'}\,\eta'_{r'}; \zeta_1 \ldots); \quad \mathfrak{G}_{\varrho-1} = (\eta'_1; \ldots \eta'_{r'}; \zeta_1 \ldots) \quad [\text{N. § 1, 5}].$$

Dabei sei

$$e_1 \neq E \ldots e_s \neq E;\ e_{s+1} = \ldots = e_r = E;\ e'_1 \neq E;\ \ldots e'_{s'} \neq E;\ e'_{s'+1} = \ldots = e'_{r'} = E,$$

wo E die Einheit des Körpers bedeutet. Dabei sind die η_i, η'_j und ζ_k untereinander linear unabhängig. Daraus folgt gruppentheoretisch

$$\mathfrak{G}^*_{\varrho-1}\,|\,\mathfrak{M}^*_{\varrho-1} = \{\eta_1\} + \ldots + \{\eta_s\}; \quad \mathfrak{G}_{\varrho-1}\,|\,\mathfrak{M}_{\varrho-1} = \{\eta'_1\} + \ldots + \{\eta'_{s'}\}.$$

Diese Summen sind direkt, $\{\eta_i\}$ und $\{\eta'_j\}$ sind zyklische Gruppen der Ordnung e_i und e'_j. Da diese Darstellung bis auf Isomorphie eindeutig ist, und da $\mathfrak{G}^*_{\varrho-1}\,|\,\mathfrak{M}^*_{\varrho-1} \sim \mathfrak{G}_{\varrho-1}\,|\,\mathfrak{M}_{\varrho-1}$ ist, so folgt $r = r'$ und $e_i = e'_i$. Die von der Einheit E verschiedenen Elementarteiler von $\mathfrak{M}^*_{\varrho-1}$ und $\mathfrak{M}_{\varrho-1}$ stimmen also miteinander überein, q. e. d.

Satz 8. *Die Basis des ϱ-ten Grundideals $\mathfrak{g}_\varrho$ von $\mathfrak{m} = (f_1 \dots f_t)$ läßt sich mit endlich vielen Schritten berechnen.*

Beweis durch vollständige Induktion.

1. $\varrho = n$. Es wird $\mathfrak{g}_n = \mathfrak{m} = (f_1 \dots f_t)$.

2. Angenommen der Satz sei bereits für $\varrho \geqq \lambda$ bewiesen. Es sei $\varrho = \lambda - 1$. Der Beweis gliedert sich in zwei Schritte.

a) Modulberechnungen.

$\mathfrak{M}^*_{\lambda-1}$ und $\mathfrak{G}^*_{\lambda-1}$ seien die in diesem Paragraphen definierten Moduln aus Linearformen in den Potenzprodukten z der $x_1 \dots x_{\lambda-1}$ mit Koeffizienten aus $\mathsf{P}[x_\lambda \dots x_n]$. Wie in Satz 6 gezeigt ist, läßt sich eine Basis von $\mathfrak{M}^*_{\lambda-1}$ mit endlich vielen Schritten berechnen. $\mathfrak{M}^{*'}_{\lambda-1}$ und $\mathfrak{G}^{*'}_{\lambda-1}$ seien Linearformenmoduln in den z mit Koeffizienten aus $\mathsf{P}[x_\lambda](x_{\lambda+1} \dots x_n)$, die die gleiche Basis haben wie $\mathfrak{M}^*_{\lambda-1}$ bzw. $\mathfrak{G}^*_{\lambda-1}$. Sie gehen also durch Adjunktion von $x_{\lambda+1} \dots x_n$ zum Körper P hervor. Nach Satz 7, 1 und Hilfssatz 4 ist $\mathfrak{G}^{*'}_{\lambda-1}$ Grundmodul von $\mathfrak{M}^{*'}_{\lambda-1}$. Es handelt sich zunächst um die Berechnung einer Basis von $\mathfrak{G}^{*'}_{\lambda-1}$.

Es sei A die Matrix der berechneten Modulbasis von $\mathfrak{M}^{*'}_{\lambda-1} = (l_1 \dots l_t)$. p sei der Rang dieses Moduls. Nach der Elementarteilertheorie gibt es dann zwei Matrizen R und S vom Range t, die eine nicht verschwindende von x_λ unabhängige t-reihige Determinante besitzen, so daß

$$R \cdot A \cdot S = \begin{Vmatrix} e_{\lambda-1,1} & 0 & \dots & 0 \\ 0 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & 0 \\ 0 & \dots & 0 & e_{\lambda-1,p} \end{Vmatrix}$$

wird. R und S lassen sich [z. B. mit den Methoden von Bôcher[11])] mit endlich vielen Schritten berechnen. Setzt man $l' = R(l)$, so bilden die l' eine neue Basis von $\mathfrak{M}^{*'}_{\lambda-1}$, da die Transformation wegen der von x_λ unabhängigen und nicht verschwindenden t-reihigen Determinante aus R umkehrbar ist. Diese neue Modulbasis besitzt die Matrix $R \cdot A$. Transformiert man ferner die Variablen z_σ der Linearformen mit S; setzt man also $z = S(z')$, so erhält die Matrix von $\mathfrak{M}^{*'}_{\lambda-1}$ die Form RAS, d. h. es wird

$$\mathfrak{M}^{*'}_{\lambda-1} = (e_{\lambda-1,1} z'_1;\ \dots e_{\lambda-1,p} z'_p).$$

Daraus ergibt sich sofort eine Basis des zugehörigen Grundmoduls

$$\mathfrak{G}^{*'}_{\lambda-1} = (z'_1;\ \dots z'_p).$$

Durch Rückgängigmachen der Transformation $z = S(z')$, das erlaubt ist,

[11]) Bôcher, Einführung in die höhere Algebra, Kap. 20.

da S eine von x_λ unabhängige, nicht verschwindende Determinante hat, erhält man für $\mathfrak{G}^{*'}_{\lambda-1}$ eine Basis in den ursprünglichen Variablen z.

$$\mathfrak{G}^{*'}_{\lambda-1} = (k_1; \ldots k_p).$$

Dabei können die k_i als Linearformen in den z mit Koeffizienten aus $\mathsf{P}[x_\lambda \ldots x_n]$ angesehen werden.

b) Berechnung von $\mathfrak{g}_{\lambda-1}$ aus $\mathfrak{G}^{*'}_{\lambda-1}$.

Da $\mathfrak{G}^{*'}_{\lambda-1}$ aus $\mathfrak{G}^{*}_{\lambda-1}$ durch Adjunktion von $x_{\lambda-1} \ldots x_n$ hervorgegangen ist, so sind die Linearformen aus $\mathfrak{G}^{*'}_{\lambda-1}$, deren Koeffizienten zu $\mathsf{P}[x_\lambda \ldots x_n]$ gehören, durch das λ-te Grundideal von $\mathfrak{g}_{\lambda-1}$, das mit $\mathfrak{g}_{\lambda-1}$ identisch ist, teilbar. Sie bestehen also aus der Gesamtheit der g, für die

$$1.\ g \equiv 0(\mathfrak{g}_{\lambda-1}). \qquad 2.\ [g] \leqq n_{\lambda-1}$$

ist. Es ist also $k_i \equiv 0(\mathfrak{g}_{\lambda-1})$ und $[k_i] \leqq n_{\lambda-1}$, wobei k_i noch ganz in den Transformationskoeffizienten angenommen werden darf. Es sei

$$|U|^\gamma k_i = U_p k_{i1} + \ldots + U_n k_{in},$$

wo die U_j Potenzprodukte der Transformationskoeffizienten $u_{\mu\nu}$ sind, während die k_{ij} nach Rücktransformation von den $u_{\mu\nu}$ unabhängig werden. Da $\mathfrak{g}_{\lambda-1}$ transformiert ist, ist also $k_{ij} \equiv 0(\mathfrak{g}_{\lambda-1})$ und es wird $[k_{ij}] \leqq n_{\lambda-1}$. Also ist

$$(k_{11} \ldots k_{pn}) \equiv 0(\mathfrak{G}^{*'}_{\lambda-1}).$$

Andererseits ist

$$\mathfrak{G}^{*'}_{\lambda-1} \equiv 0(k_{11} \ldots k_{pn}).$$

Also wird

$$\mathfrak{G}^{*'}_{\lambda-1} = (k_{11} \ldots k_{pn}).$$

Man setze nun für die z_σ wieder die Potenzprodukte in $x_1 \ldots x_{\lambda-1}$ und fasse $\mathfrak{k} = (k_{11} \ldots k_{pn})$ auf als Ideal in $\mathsf{P}[x_1 \ldots x_n]$, das nach Konstruktion seiner Basis transformiert ist.

Es sei

$$g \equiv 0(\mathfrak{g}_{\lambda-1}).$$

Da nach der Folgerung aus Satz 6 $\mathfrak{G}^{*}_{\lambda-1}$ und somit auch $\mathfrak{G}^{*'}_{\lambda-1}$ bereits eine Basis von $\mathfrak{g}_{\lambda-1}$ enthält, so gibt es ein $a^{(\lambda+1)} \neq 0$, so daß

$$a^{(\lambda+1)} g \equiv 0(\mathfrak{k})$$

wird. Ist umgekehrt

$$a^{(\lambda+1)} g \equiv 0(\mathfrak{k}),$$

so ist

$$g \equiv 0(\mathfrak{g}_{\lambda-1}).$$

Das heißt also, da $\mathfrak{k}$ transformiert ist, $\mathfrak{g}_{\lambda-1}$ ist das λ-te Grundideal von $\mathfrak{k}$. Nach Voraussetzung läßt sich nun das λ-te Grundideal stets mit endlich vielen Schritten berechnen. Es läßt sich also auch $\mathfrak{g}_{\lambda-1}$ und damit jedes Grundideal von $\mathfrak{m}$ mit endlich vielen Schritten berechnen, q. e. d.

Zusatz zu Satz 8. Man setze

$$E_{\varrho-1}^{(\varrho)} = e_{\varrho-1,p}; \qquad R_{\varrho-1}^{(\varrho)} = \prod_{i=1}^{p} e_{\varrho-1,i}.$$

Ohne Beschränkung der Allgemeinheit kann man $E_{\varrho-1}^{(\varrho)}$ und $R_{\varrho-1}^{(\varrho)}$ als ganz und primitiv in $x_{\varrho-1} \ldots x_n$ annehmen. Dann wird

$$E = \prod_{\varrho=1}^{n} E_{\varrho-1}^{(\varrho)}$$

die *Elementarteilerform* von $\mathfrak{m}$ und

$$R = \prod_{\varrho=1}^{n} R_{\varrho-1}^{(\varrho)}$$

die *Norm* von $\mathfrak{m}$.

Damit sind also diese beiden für die Charakterisierung des Ideals durch seine Nullstellen wichtigen Polynome gewonnen.

Nach N. Satz 11 läßt die Norm von $\mathfrak{m}$ eine Zerlegung zu

$$\begin{aligned} R &= \prod_{i,\nu} (x_i - t_{1i}\,\bar{y}_{1\nu} - \ldots - t_{ni}\,\bar{y}_{n\nu})^{\delta} \\ &= \prod_{i,\nu} (t_{1i}(y_1 - \bar{y}_{1\nu}) + \ldots + t_{ni}(y_n - \bar{y}_{n\nu}))^{\delta}. \end{aligned}$$

Dabei bedeuten die t_{ij} die Koeffizienten der Umkehrtransformation U^{-1} und die $\bar{y}_{1\nu} \ldots \bar{y}_{n\nu}$ durchlaufen ein von den t_{ij} unabhängiges vollständiges Nullstellensystem des nicht transformierten Ideals $\overline{\mathfrak{m}}$. Nach § 2 läßt sich die angegebene Zerlegung der Norm und damit die Berechnung des vollständigen Nullstellensystems mit endlich vielen Schritten durchführen.

§ 7.

Primideale.

Während die bisherigen Methoden, mit Ausnahme der Zerlegung der Polynome in § 2 auf die besonderen Eigenschaften des zugrunde gelegten Körpers gar keine Rücksicht zu nehmen brauchten, wird es für die Berechnung der zu $\mathfrak{m}$ gehörigen Primideale wesentlich, ob der Körper vollkommen oder unvollkommen ist. Der Grund dafür liegt in den § 1, 5 zitierten Sätzen, nach denen man bei zugrunde gelegtem vollkommenem Körper aus der Tatsache, daß die Elementarteilerform Primfunktion ist, schließen kann, daß das Ideal Primideal ist, während im unvollkommenen Körper dieser Schluß unzulässig ist. Da uns nun nach dem bisher Berechneten die Elementarteilerformen der gesuchten Primideale als Primfaktoren der Norm bekannt sind [N. Satz 10], wir aber weiter nichts von diesen Primidealen kennen, so wird die Berechnung ihrer Basis von ihrer Elementarteilerform ausgehen müssen, und es wird sich damit ein Gegen-

satz zwischen der Berechnung der Primideale im vollkommenen und im unvollkommenen Körper ergeben. Satz 9 wird die Methoden bringen, die in beiden Fällen zur Anwendung kommen. Im Fall des vollkommenen Körpers wird damit alles erledigt sein, für den Fall des unvollkommenen Körpers ist noch eine weitere Rechnung nötig, die in Satz 10 gebracht wird. Satz 11 faßt dann beides zusammen und wendet die gefundenen Methoden auf die speziellen Primideale des gegebenen Ideals an.

Satz 9. Voraussetzung. *Es sei die Primfunktion $P^{(\varrho)}$ Elementarteilerform des transformierten Primideals $\mathfrak{p}$ der Dimension $n-\varrho$ in $\mathsf{P}[x_1 \dots x_n] = \overline{\mathsf{P}}(u)[x_1 \dots x_n]$. P sei das daraus durch Rücktransformation $x = U^{-1}(y)$ und Multiplikation mit $|U|^\gamma = |u_{\mu\nu}|^\gamma$ hervorgehende Polynom, das ganz ist in den $u_{\mu\nu}$. Es sei*

$$P = \sum_{\lambda=1}^{l} U_\lambda P_\lambda .$$

Dabei seien die U_λ Potenzprodukte der Transformationskoeffizienten $u_{\mu\nu}$ und die P_λ Größen aus $\overline{\mathsf{P}}[y_1 \dots y_n]$. Dann ist

$$\bar{\mathfrak{r}} = (P_1 \dots P_l)$$

Ideal in $\overline{\mathsf{P}}[y_1 \dots y_n]$; $\mathfrak{r}$ sei das daraus durch Transformation hervorgehende transformierte Ideal, $\mathfrak{p}'$ das ϱ-te Grundideal von $\mathfrak{r}$.

Behauptung. $\mathfrak{p} = \mathfrak{p}'$, *falls $\overline{\mathsf{P}}$ ein vollkommener Körper ist. Sonst gilt nur: $\mathfrak{p}'$ ist ein zu $\mathfrak{p}$ gehörendes Primärideal.*

Beweis. Wegen $P^{(\varrho)} \equiv 0(\mathfrak{r})$ ist das 1-te bis $\varrho - 1$-te Grundideal von $\mathfrak{r}$ gleich dem Einheitsideal $\mathfrak{o}$. Wegen $\mathfrak{r} \equiv 0(\mathfrak{p}')$ gilt daselbe für $\mathfrak{p}'$. Da aber $\mathfrak{p}'$ das ϱ-te Grundideal von $\mathfrak{r}$ ist, so ist es mit seinem ϱ-ten Grundideal identisch. $\mathfrak{p}'$ hat also nur einen von der Einheit verschiedenen höchsten Elementarteiler, alle zu $\mathfrak{p}'$ gehörenden Primideale sind von der Dimension $n - \varrho$.

Da nun $P^{(\varrho)} \equiv 0(\mathfrak{p}')$ ist, so ist $P^{(\varrho)}$ ein Vielfaches der Elementarteilerform von $\mathfrak{p}'$, die infolgedessen, da $P^{(\varrho)}$ Primfunktion ist, entweder $P^{(\varrho)}$ oder die Einheit E ist.

Angenommen die Elementarteilerform von $\mathfrak{p}'$ wäre E. Dann wäre $\mathfrak{p}' = \mathfrak{o}$; d. h. es gäbe ein Polynom

$$G^{(\varrho+1)} \neq 0,$$

so daß

$$G^{(\varrho+1)} \equiv 0(\mathfrak{r})$$

wäre.

Nach Definition von $\bar{\mathfrak{r}}$ folgt aus $P^{(\varrho)} \equiv 0(\mathfrak{p})$, sicher $\bar{\mathfrak{r}} \equiv 0(\bar{\mathfrak{p}})$, wo $\bar{\mathfrak{p}}$ das zu $\mathfrak{p}$ gehörende nicht transformierte Ideal ist. Also ist auch $\mathfrak{r} \equiv 0(\mathfrak{p})$. Es wäre also

$$G^{(\varrho+1)} \equiv 0(\mathfrak{p}).$$

$\mathfrak{p}$ wäre also entgegen der Voraussetzung höchstens von der Dimension $n-\varrho-1$. Also war die Annahme falsch, und $P^{(\varrho)}$ ist die Elementarteilerform von $\mathfrak{p}'$.

Ist nun $\bar{\mathsf{P}}$ ein vollkommener Körper, so ist $\mathfrak{p}'$ nach N. Satz 13 ein Primideal, dessen Elementarteilerform mit dem von $\mathfrak{p}$ übereinstimmt. Da durch die Elementarteilerform die Nullstellen des Ideals bestimmt sind, so haben die beiden Primideale dieselben Nullstellen, sind also identisch. Ist $\bar{\mathsf{P}}$ unvollkommen, so kann man nur schließen, daß $\mathfrak{p}'$ Primärideal ist. Da $\mathfrak{p}'$ dieselben Nullstellen hat wie $\mathfrak{p}$, so ist $\mathfrak{p}$ das zu $\mathfrak{p}'$ gehörende Primideal, q. e. d.

Zusatz. Daß im Fall des unvollkommenen Körpers $\mathfrak{p}'$ ein eigentliches Primärideal werden kann, zeigt das in N. § 6 zum Schluß gebrachte Beispiel.

Es sei $\bar{\mathsf{P}}$ der Restklassenkörper mod 2, dem die Unbestimmte λ adjungiert ist. $n=2$. Es sei $\bar{\mathfrak{p}}=(y_1^2+\lambda;\ y_1+y_2)$ das nichttransformierte Ideal. Es ist also $\mathfrak{p}=((u_{11}x_1+u_{12}x_2)^2+\lambda;\ x_1(u_{11}+u_{21})+x_2(u_{12}+u_{22}))$. Als Elementarteilerform ergibt sich

$$P^{(2)}=x_2^2+\lambda(t_{12}^2+t_{22}^2).$$

Dabei sind die t_{ij} Koeffizienten der Umkehrtransformation U^{-1}. Ideale, die $P^{(3)}$ zum ersten von der Einheit verschiedenen Elementarteiler haben, haben $P^{(2)}$ als einzigen Elementarteiler, da $n=2$ ist. Da $P^{(2)}$ Primfunktion ist, sind also diese Ideale Primärideale. In den Bezeichnungen des Satzes 9 wird also $\mathfrak{r}=\mathfrak{p}'$. Durch $x=U^{-1}(y)$ erhält man aus $P^{(2)}$

$$P=t_{12}^2(y_1^2+\lambda)+t_{22}^2(y_2^2+\lambda).$$

$\mathfrak{p}'$ entsteht also durch $y=U(x)$ aus dem Ideal

$$((y_1^2+\lambda);(y_2^2+\lambda))=(y_1^2+\lambda;(y_1+y_2)^2).$$

Das aber ist, wie man sofort sieht, ein zu $\bar{\mathfrak{p}}$ gehörendes echtes Primärideal, da es $(y_1+y_2)^2$, aber nicht (y_1+y_2) enthält. Das entsprechende gilt natürlich für das transformierte Ideal.

Zum Beweis des Satzes 10 sind nun zwei Hilfssätze nötig.

Hilfssatz 5. Voraussetzung. $\mathfrak{q}$ *sei ein Ideal in* $\mathfrak{R}=\mathsf{P}[x_1\dots x_n]$. *Dabei sei* x_i *algebraisch oder transzendent in bezug auf* $\mathsf{P}[x_1\dots x_{i-1}]$. $\mathfrak{q}'$ *sei das Ideal in* $\mathsf{P}(x_n)[x_1\dots x_{n-1}]$, *dessen Basiselemente mit denen von* $\mathfrak{q}$ *übereinstimmen. Die zu* $\mathfrak{q}'$ *gehörenden Größen aus* $\mathsf{P}[x_1\dots x_n]$ *sollen durch* $\mathfrak{q}$ *teilbar sein.* Dann sind $\mathfrak{q}$ und $\mathfrak{q}'$ eindeutig durcheinander bestimmt.

Behauptung. *Mit* $\mathfrak{q}$ *ist* $\mathfrak{q}'$ *Primideal bzw. Primärideal und umgekehrt.*

Beweis. 1. $\mathfrak{q}$ sei Primärideal.

Es sei $a' \cdot b' \equiv 0 (\mathfrak{q}')$, aber $b'^{\varkappa} \not\equiv 0 (\mathfrak{q}')$ für jedes $\varkappa$. Dann gibt es Polynome $f(x_n)$ und $g(x_n)$, so daß

$$f \cdot a' \equiv 0 (\mathsf{P}[x_1 \dots x_n]) \quad \text{und} \quad g \cdot b' \equiv 0 (\mathsf{P}[x_1 \dots x_n]).$$

Es wird also

$$f \cdot a' \cdot g \cdot b' \equiv 0 (\mathfrak{q}).$$

Da aber aus

$$g^{\varkappa} \cdot b'^{\varkappa} \equiv 0 (\mathfrak{q})$$

direkt $b'^{\varkappa} \equiv 0 (\mathfrak{q}')$ folgen würde, so ist

$$(g \cdot b')^{\varkappa} \not\equiv 0 (\mathfrak{q})$$

für jedes $\varkappa$. Da $\mathfrak{q}$ primär ist, folgt

$$f \cdot a' \equiv 0 (\mathfrak{q})$$

und somit

$$a' \equiv 0 (\mathfrak{q}'),$$

d. h. $\mathfrak{q}'$ ist primär.

2. $\mathfrak{q}'$ sei Primärideal.

Aus

$$a \cdot b \equiv 0 (\mathfrak{q}); \qquad b^{\varkappa} \not\equiv 0 (\mathfrak{q})$$

für jedes $\varkappa$ folgt

$$a \cdot b \equiv 0 (\mathfrak{q}'); \qquad b^{\varkappa} \not\equiv 0 (\mathfrak{q}')$$

für jedes $\varkappa$. Nach Voraussetzung wird also

$$a \equiv 0 (\mathfrak{q}')$$

und somit auch

$$a \equiv 0 (\mathfrak{q}),$$

d. h. $\mathfrak{q}$ ist Primärideal.

Setzt man in diesem Beweis für $\varkappa$ stets 1, so ergibt sich: mit $\mathfrak{q}$ ist $\mathfrak{q}'$ Primideal und umgekehrt, q. e. d.

Hilfssatz 6. Voraussetzung. $\mathfrak{q}$ *sei ein Ideal in* $\mathsf{P}[x_1 \dots x_n]$. *Dabei sei* x_i $[i = 1 \dots n]$ *transzendent in bezug auf* $\mathsf{P}[x_1 \dots x_{i-1}]$. $P^{(n)}(x_n)$ *sei Primfunktion und es gelte*

$$P^{(n)}(x_n) \equiv 0 (\mathfrak{q}).$$

ξ_n *sei algebraisch in bezug auf* P *und zwar sei*

$$P^{(n)}(\xi_n) = 0.$$

$\mathsf{P}[x_1 \dots x_{n-1} \xi_n]$ wird also ein Ring ohne Nullteiler sein. $\mathfrak{q}'$ *sei das Ideal in* $\mathsf{P}[x_1 \dots x_{n-1} \xi_n]$, *dessen Basiselemente aus denen von* $\mathfrak{q}$ *durch Vertauschen von* x_n *mit* ξ_n *hervorgehen.* Die Basiselemente von $\mathfrak{q}$ gehen dann umgekehrt aus denen von $\mathfrak{q}'$ hervor durch Vertauschen von ξ_n mit x_n und durch Hinzufügen von $P^{(n)}(x_n)$ zur Basis.

Behauptung. *Mit* $\mathfrak{q}$ *ist* $\mathfrak{q}'$ *Primideal bzw. Primärideal und umgekehrt.*

Beweis. Der Beweis läßt sich direkt entsprechend dem Beweis von Hilfssatz 5 durch Rechnung führen. Er ergibt sich aber auch durch folgende Überlegung: $\mathfrak{q}$ ist dann und nur dann prim bzw. primär, wenn dasselbe für den Ring $\mathfrak{o}|\mathfrak{q}$ gilt, d. h. wenn dieser keine Nullteiler hat bzw. wenn eine Potenz jedes Nullteilers verschwindet. Die Vertauschung von x_n mit ξ_n bedeutet Übergang zu den Restklassen nach $(P^{(n)}(x_n))$. Dabei wird

$$\mathfrak{o}|(P^{(n)}(x_n)) = \mathfrak{o}', \qquad \mathfrak{q}|(P^{(n)}(x)) = \mathfrak{q}'.$$

Bekanntlich sind nun $\mathfrak{o}|\mathfrak{q}$ und $\mathfrak{o}'|\mathfrak{q}'$ isomorph. (Aufgelöst nach Elementen in $\mathfrak{o}$ enthalten die beiden Nullklassen dieselben Elemente.) Mit $\mathfrak{o}|\mathfrak{q}$ ist also $\mathfrak{o}'|\mathfrak{q}'$ prim bzw. primär, d. h. mit $\mathfrak{q}$ ist $\mathfrak{q}'$ Prim- bzw. Primärideal und umgekehrt, q. e. d.

Satz 10. Voraussetzung. $\mathfrak{q}$ *sei ein Primärideal in* $\mathsf{P}[x_1 \dots x_n]$, *dessen Elementarteilerform* $P^{(\varrho)}$ *Primfunktion ist.* $\mathfrak{q}$ ist also Primideal, falls P vollkommen ist.

Behauptung. *Eine Basis des zu* $\mathfrak{q}$ *gehörigen Primideals* $\mathfrak{p}$ *läßt sich stets mit endlich vielen Schritten berechnen.*

Beweis durch vollständige Induktion.

E sei die Einheit von P. Dann kann $P^{(\varrho)} \neq E$ angenommen werden, da sonst $\mathfrak{q} = \mathfrak{p} = \mathfrak{o}$ ist.

1. $n = 1$. $\mathfrak{q}$ ist Hauptideal. $\mathfrak{q} = (Q)$. Aus $P^{(\varrho)} \equiv 0\,(\mathfrak{q})$ folgt $P^{(\varrho)} \equiv 0\,(Q)$. Also ist entweder $Q = P^{(\varrho)}$ oder $Q = E$, da $P^{(\varrho)}$ Primfunktion ist. Es ist aber $Q \neq E$, da sonst $\mathfrak{q} = \mathfrak{o}$ wäre, entgegen der Voraussetzung, daß $P^{(\varrho)} \neq E$ die Elementarteilerform ist. Also ist $\mathfrak{q} = (P^{(\varrho)})$. Da $P^{(\varrho)}$ Primfunktion ist, ist also auch $\mathfrak{q}$ Primideal.

2. Angenommen der Satz sei für $n = r - 1$ bereits bewiesen. Es sei $n = r$. Wie in § 1 gezeigt wurde, genügt es, den Satz für transformierte Ideale zu beweisen, weil damit die eindeutige Berechnung des Primideals für nicht transformierte $\mathfrak{q}$ mitgegeben ist. $\mathfrak{q}$ sei also im folgenden transformiert.

a) $\mathfrak{q}$ sei von höherer als 0-ter Dimension. $\varrho \neq r$. $\mathfrak{q}'$ sei das aus $\mathfrak{q}$ durch Adjunktion von x_r hervorgegangene Ideal in $\mathsf{P}(x_r)[x_1 \dots x_{r-1}]$. Die zu $\mathsf{P}[x_1 \dots x_r]$ gehörenden Polynome aus $\mathfrak{q}'$ bilden dann das $r-1$-te Grundideal von $\mathfrak{q}$, das mit $\mathfrak{q}$ übereinstimmt, da $\mathfrak{q}$ mindestens von der 1-ten Dimension ist. Nach Hilfssatz 5 ist $\mathfrak{q}'$ ein Primärideal in $\mathsf{P}(x_r)[x_1 \dots x_{r-1}]$. Da die Nullstellen von $\mathfrak{q}$ mit denen von $\mathfrak{q}'$ übereinstimmen, so ist die Elementarteilerform von $\mathfrak{q}'$ eine zu $P^{(\varrho)}$ gehörende

Primärfunktion, die wegen $P^{(\varrho)} \equiv 0 (\mathfrak{q}')$ mit $P^{(\varrho)}$ identisch ist. Nach Voraussetzung lassen sich also die Basiselemente des zu $\mathfrak{q}'$ gehörigen Primideals mit endlich vielen Schritten berechnen. Es sei $\mathfrak{p}' = (p_1 \dots p_\nu)$, wobei die p_i $[i = 1 \dots \nu]$ als Größen aus $\mathsf{P}[x_1 \dots x_r]$ angenommen werden dürfen.

$\mathfrak{p}$ enthalte alle und nur die Polynome aus $\mathfrak{p}'$, die zu $\mathsf{P}[x_1 \dots x_r]$ gehören. Nach Hilfssatz 5 ist $\mathfrak{p}$ Primideal. Aus

$$\mathfrak{q}' \equiv 0 (\mathfrak{p}') \quad \text{und} \quad \mathfrak{p}'^{\varkappa} \equiv 0 (\mathfrak{q}')$$

folgt auch

$$\mathfrak{q} \equiv 0 (\mathfrak{p}) \quad \text{und} \quad \mathfrak{p}^{\varkappa} \equiv 0 (\mathfrak{q}),$$

denn Teilbarkeiten bleiben bei der Adjunktion von x_r erhalten, und wenn das Ideal $\mathfrak{k}$ aus der Gesamtheit der in $\mathsf{P}[x_1 \dots x_r]$ liegenden Polynome aus $\mathfrak{p}'^{\varkappa}$ besteht, so ist sicher $\mathfrak{p}^{\varkappa} \equiv 0 (\mathfrak{k})$, da alle durch $\mathfrak{p}$ teilbaren Polynome auch durch $\mathfrak{p}'$ teilbar sind.

$\mathfrak{p}$ ist also das zu $\mathfrak{q}$ gehörige Primideal, also ist $\mathfrak{p}$ transformiert. Aus den Basiselementen von $\mathfrak{p}'$ soll jetzt eine Basis von $\mathfrak{p}$ berechnet werden. Ist $p \equiv 0 (\mathfrak{p})$ und $|U|^{\gamma} p = U_1 p_1 + \dots + U_\mu p_\mu$ eine Aufspaltung von p in transformierte Bestandteile p_i, so daß die U_i Potenzprodukte der Transformationskoeffizienten sind, und die p_i nach Rücktransformation von diesen unabhängig werden, so gilt, da $\mathfrak{p}$ transformiert ist, $p_i \equiv 0 (\mathfrak{p})$, also auch $p_i \equiv 0 (\mathfrak{p}')$. Die Basiselemente $(p_1 \dots p_\nu)$ von $\mathfrak{p}'$ können also bereits so gewählt werden, daß sie nach Rücktransformation von den Transformationskoeffizienten unabhängig werden. $(p_1 \dots p_\nu)$ ist dann in $\mathsf{P}[x_1 \dots x_r]$ ein transformiertes Ideal, die Gesamtheit aller zu $\mathsf{P}[x_1 \dots x_r]$ gehörenden Polynome aus $\mathfrak{p}'$, also die Elemente von $\mathfrak{p}$ bilden dann das $r-1$-te Grundideal von $(p_1 \dots p_\nu)$, das sich nach Satz 8 mit endlich vielen Schritten berechnen läßt.

b) $\mathfrak{q}$ sei von der Dimension 0. Die Primfunktion $P^{(r)}(x_r)$ ist dann Funktion von x_r allein. ξ_r sei eine durch die Gleichung $P^{(r)}(\xi_r) = 0$ algebraisch von P abhängende Größe. $\mathfrak{q}'$ sei das aus $\mathfrak{q}$ durch den Übergang zum Restklassensystem nach $P^{(r)}(x_r)$ hervorgehende Ideal in $\mathsf{P}[x_1 \dots x_{r-1} \xi_r]$, das aus $\mathfrak{q}$ durch Vertauschen von x_r mit ξ_r entsteht. Nach Hilfssatz 6 ist $\mathfrak{q}'$ Primärideal. Durch Adjunktion von ξ_r zum Körper P geht $\mathfrak{q}'$ über in ein Ideal $\mathfrak{q}''$. Die Gesamtheit der in bezug auf ξ_r ganzen Polynome aus $\mathfrak{q}''$ ist durch $\mathfrak{q}'$ teilbar. Ist nämlich

$$g(x_1 \dots x_{r-1} \xi_r) \equiv 0 (\mathfrak{q}''),$$

so folgt

$$F(\xi_r)\, g(x_1 \dots x_{r-1} \xi_r) \equiv 0 (\mathfrak{q}').$$

Dabei ist

$$F(\xi_r) \neq 0.$$

Daraus folgt

$$F(x_r)\,g(x_1 \ldots x_{r-1}\,x_r) \equiv 0\,(\mathfrak{q})$$

und

$$F(x_r) \not\equiv 0\,(P^{(r)}(x_r)).$$

Da $P^{(r)}(x_r)$ Primfunktion ist, folgt daraus $F^{\varkappa}(x_r) \not\equiv 0\,(P^{(r)}(x_r))$ für jedes $\varkappa$. Da $P^{(r)}(x_r)$ als Elementarteilerform von $\mathfrak{q}$ der größte gemeinsame Teiler aller nur von x_r abhängenden Polynome aus $\mathfrak{q}$ ist, so folgt $F^{\varkappa}(x_r) \not\equiv 0\,(\mathfrak{q})$ für jedes $\varkappa$. Also ist $g(x_1 \ldots x_{r-1}\,x_r) \equiv 0\,(\mathfrak{q})$ und somit auch $g(x_1 \ldots x_{r-1}\,\xi_r) \equiv 0\,(\mathfrak{q}')$. Nach Hilfssatz 5 ist $\mathfrak{q}''$ also Primärideal.

Die Elementarteilerform von $\mathfrak{q}''$ ist eine, und zwar nicht immer die erste Potenz einer Primfunktion. Nach Satz 1 läßt sich mit endlich vielen Schritten die zugehörige Primfunktion berechnen, nach Satz 9 findet man die Basis eines Primärideals $\mathfrak{q}'''$, dessen Elementarteilerform diese Primfunktion ist, das also zu demselben Primideal gehört wie $\mathfrak{q}''$. Nach Voraussetzung läßt sich das zu $\mathfrak{q}'''$ und somit zu $\mathfrak{q}''$ gehörende Primideal $\mathfrak{p}''$ mit endlich vielen Schritten berechnen.

Es sei $\mathfrak{p}'' = (p_1(x_1 \ldots x_{r-1}\,\xi_r) \ldots p_\nu(x_1 \ldots x_{r-1}\,\xi_r))$. Ohne Beschränkung der Allgemeinheit können die p_i als ganz in ξ_r angenommen werden.

$$\begin{aligned} |U|^{\gamma_i} p_i(x_1 \ldots x_{r-1}\,x_r) &= U_1\,p_{i1}(x_1 \ldots x_r) + \ldots + U_\mu\,p_{i\mu}(x_1 \ldots x_r), \\ |U|^{\gamma} P^{(r)}(x_r) &= U_1\,P_1(x_1 \ldots x_r) + \ldots + U_\mu\,P_\mu(x_1 \ldots x_r) \end{aligned}$$

sei die Aufspaltung dieser Polynome in transformierte Bestandteile. Es sei $\mathfrak{p}' = (p_{11}(x_1 \ldots x_r) \ldots p_{\nu\mu}(x_1 \ldots x_r),\ P_1(x_1 \ldots x_r) \ldots P_\mu(x_1 \ldots x_r))$ ein Ideal in $\mathsf{P}[x_1 \ldots x_r]$. Nach Konstruktion ist $\mathfrak{p}'$ sicher ein transformiertes Ideal. Es wird sich zeigen, daß $\mathfrak{p}'$ bereits das gesuchte zu $\mathfrak{q}$ gehörende Primideal $\mathfrak{p}$ ist. Es wird nämlich:

1. $\mathfrak{p}' \equiv 0\,(\mathfrak{p})$, denn aus

$$p_i(x_1 \ldots x_{r-1}\,\xi_r) \equiv 0\,(\mathfrak{p}'')$$

folgt

$$p_i^{\varkappa}(x_1 \ldots x_{r-1}\,\xi_r) \equiv 0\,(\mathfrak{q}'').$$

Nach dem über $\mathfrak{q}''$ Bewiesenen folgt daraus

$$p_i^{\varkappa}(x_1 \ldots x_{r-1}\,x_r) \equiv 0\,(\mathfrak{q}),$$

also wird

$$p_i(x_1 \ldots x_{r-1}\,x_r) \equiv 0\,(\mathfrak{p}).$$

Da ferner $P^{(r)}(x_r) \equiv 0\,(\mathfrak{p})$ ist, und da $\mathfrak{p}$ als transformiertes Ideal mit einem Polynom auch dessen transformierte Bestandteile enthält, so ist $\mathfrak{p}' \equiv 0\,(\mathfrak{p})$.

2. $\mathfrak{p}'$ ist Primärideal. Da $\mathfrak{p}'$ transformiert ist, folgt nämlich aus $P^{(r)}(x_r) \equiv 0\,(\mathfrak{p}')$, daß $\mathfrak{p}'$ höchstens von der Dimension 0 ist, aus $\mathfrak{p} \neq o$ und $\mathfrak{p}' \equiv 0\,(\mathfrak{p})$, daß es genau von der Dimension 0 ist. Da $P^{(r)}(x_r)$

Primfunktion ist, ist sie mithin die Elementarteilerform von $\mathfrak{p}'$. $\mathfrak{p}'$ ist also Primärideal, und $P^{(r)}(x_r)$ ist der größte gemeinsame Teiler aller nur von x_r abhängenden Polynome aus $\mathfrak{p}'$.

3. $\mathfrak{p} \equiv 0\,(\mathfrak{p}')$. Es sei nämlich $p(x_1 \ldots x_{r-1}\, x_r) \equiv 0\,(\mathfrak{p})$. Entweder ist $p(x_1 \ldots x_{r-1}\, x_r) \equiv 0\,(P^{(r)}(x))$, dann ist sicher $p(x_1 \ldots x_{r-1}\, x_r) \equiv 0\,(\mathfrak{p}')$. Oder es ist $p(x_1 \ldots x_{r-1}\, x_r) \not\equiv 0\,(P^{(r)}(x_r))$, dann ist $p(x_1 \ldots x_{r-1}\, \xi_r) \equiv 0\,(\mathfrak{p}'')$. Dann aber gibt es ein $F(x_r)$, so daß $F(x_r) \cdot p(x_1 \ldots x_{r-1}\, x_r) \equiv 0\,(\mathfrak{p}')$ und $F(x_r) \not\equiv 0\,(P^{(r)}(x_r))$ wird. Es wird also auch $F^{\varkappa}(x_r) \not\equiv 0\,(P^{(r)}(x_r))$ für jedes $\varkappa$ und somit wird nach dem unter 2 bemerkten $F(x_r) \not\equiv 0\,(\mathfrak{p}')$ für jedes $\varkappa$. Da $\mathfrak{p}'$ Primärideal ist, folgt daraus $p(x_1 \ldots x_{r-1}\, x_r) \equiv 0\,(\mathfrak{p}')$ und somit $\mathfrak{p} \equiv 0\,(\mathfrak{p}')$.

Aus 1 und 3 ergibt sich $\mathfrak{p} = \mathfrak{p}'$. Mit der Basis von $\mathfrak{p}'$ ist also auch die von $\mathfrak{p}$ bekannt, q. e. d.

Satz 11. *Die zu einem Ideal* $\mathfrak{m}$ *gehörigen Primideale lassen sich mit endlich vielen Schritten berechnen.*

Beweis. Nach N. Satz 10 sind die Elementarteilerformen der zu $\mathfrak{m}$ gehörigen Primideale die Primfunktionen, die zu den Primärfaktoren der Einzelnormen $\mathfrak{N}^{(i)}$ von $\mathfrak{m}$ gehören. Satz 8 erlaubt die Berechnung der $\mathfrak{N}^{(i)}$ mit endlich vielen Schritten, § 2 gibt Methoden zur Berechnung der zugehörigen Primfaktoren. Nach Satz 9 läßt sich zu jeder solchen Primfunktion ein Ideal berechnen, das im vollkommenen Körper das zu $\mathfrak{m}$ gehörende Primideal, im unvollkommenen Körper jedenfalls ein zu diesem Primideal gehörendes Primärideal ist, dessen Elementarteilerform Primfunktion ist. Nach Satz 10 läßt sich das zugehörige Primideal auch in diesem Fall berechnen. Die Sätze 9 und 10 liefern also die Methoden, nach denen man mit endlich vielen Schritten die Primideale finden kann.

§ 8.

Primärideale und isolierte Komponenten.

Die Primärideale, die in einer Darstellung von $\mathfrak{m}$ als kleinstes gemeinsames Vielfaches größter primärer Komponenten auftreten, sind nicht eindeutig. Es kann sich also nur um die Berechnung irgendeines bei einer solchen Darstellung möglichen Systems primärer Ideale handeln.

Es sei $\mathfrak{p}_{\varrho\sigma}$ ein zu $\mathfrak{m}$ gehöriges Primideal $n - \varrho$-ter Dimension. Ist λ größer als der Exponent irgendeines zu $\mathfrak{p}_{\varrho\sigma}$ gehörigen Primärideals $\mathfrak{q}$, das in einer Darstellung von $\mathfrak{m}$ auftreten kann, so ist das ϱ-te Grundideal von $(\mathfrak{m}, \mathfrak{p}_{\varrho\sigma}^{\lambda})$ auch ein solches. Zur Berechnung der Primärideale genügt also die Auffindung einer oberen Schranke für λ. Es wird sich zeigen, daß die Zahl $\varkappa(t, q, n)$, die im Hentzeltschen Nullstellensatz berechnet wurde, eine solche Schranke ist.

Diese Schranke greift nun allerdings viel höher, als es nötig ist. Das zeigt das einfache Beispiel

$$\mathfrak{m} = (x^2; x \cdot y) = [(x); (x^2; y)].$$

Die zu $\mathfrak{m}$ gehörigen Primideale sind (x) und $(x; y)$. Die Exponenten der auftretenden Primärideale sind also alle höchstens 2. $\lambda = 2$ genügt also für den vorliegenden Fall. Satz 5 liefert dagegen $\varkappa(2, 2, 2) = 256$.

Satz 12. Voraussetzung. $\mathfrak{p}_{\varrho 1} \dots \mathfrak{p}_{\varrho m_\varrho}$ $[\varrho = 1 \dots n]$ *seien die zu* $\mathfrak{m}$ *gehörenden Primideale* $n - \varrho$*-ter Dimension.* $\varkappa = \varkappa(t, q, n)$ *sei die in Satz* 5 *berechnete Zahl.* $\mathfrak{q}_{\varrho\sigma}$ *sei das* ϱ*-te Grundideal von* $(\mathfrak{m}, \mathfrak{p}_{\varrho\sigma}^{\varkappa})$. $\mathfrak{q}_{\varrho\sigma}$ *ist also Primärideal und gehört zu* $\mathfrak{p}_{\varrho\sigma}$. *Als Grundideal eines transformierten Ideals ist es selbst transformiert.*

Behauptung. $\mathfrak{m} = [\mathfrak{q}_{11} \dots \mathfrak{q}_{nm_n}]$.

Beweis. Es sei $\xi_{\varrho\sigma}^1 \dots \xi_{\varrho\sigma}^n$ Nullstelle vom Transzendenzgrad $n - \varrho$ des Primideals $\mathfrak{p}_{\varrho\sigma}$. Die $\xi_{\varrho\sigma}^{\varrho+1} \dots \xi_{\varrho\sigma}^n$ sind also transzendent in bezug auf P.

$\mathfrak{o}_{\varrho\sigma} = (x_1 - \xi_{\varrho\sigma}^1 \dots x_n - \xi_{\varrho\sigma}^n)$ ist dann das zu dieser Nullstelle gehörende Nullstellenideal, es ist Primideal 0-ter Dimension in $\mathsf{P}(\xi_{\varrho\sigma}^1 \dots \xi_{\varrho\sigma}^n)[x_1 \dots x_n]$, und es wird

$$\mathfrak{p}_{\varrho\sigma} \equiv 0\,(\mathfrak{o}_{\varrho\sigma}),$$

also auch

$$(\mathfrak{m}, \mathfrak{p}_{\varrho\sigma}^{\varkappa}) \equiv 0\,(\mathfrak{m}, \mathfrak{o}_{\varrho\sigma}^{\varkappa}).$$

Um Satz 5 anzuwenden, ist nur zu zeigen, daß das Grundideal $\mathfrak{q}_{\varrho\sigma}$ durch $(\mathfrak{m}, \mathfrak{o}_{\varrho\sigma}^{\varkappa})$ teilbar ist.

Da $(\mathfrak{m}, \mathfrak{o}_{\varrho\sigma}^{\varkappa}) \equiv 0\,(\mathfrak{o}_{\varrho\sigma})$ und $\mathfrak{o}_{\varrho\sigma}^{\varkappa} \equiv 0\,(\mathfrak{m}, \mathfrak{o}_{\varrho\sigma}^{\varkappa})$ ist, und da $\mathfrak{o}_{\varrho\sigma}$ die Dimension 0 hat, so ist $(\mathfrak{m}, \mathfrak{o}_{\varrho\sigma}^{\varkappa})$ ein zu $\mathfrak{o}_{\varrho\sigma}$ gehörendes Primärideal.

$(\mathfrak{m}, \mathfrak{o}_{\varrho\sigma}^{\varkappa})$ enthält kein von $x_1 \dots x_\varrho$ freies, von 0 verschiedenes Polynom. Ist nämlich $G^{(\varrho+1)}(x_{\varrho+1} \dots x_n) \not\equiv 0$, so ist, da $\xi_{\varrho\sigma}^{\varrho+1} \dots \xi_{\varrho\sigma}^n$ transzendent in bezug auf P sind, $G^{(\varrho+1)}(\xi_{\varrho\sigma}^{\varrho+1} \dots \xi_{\varrho\sigma}^n) \neq 0$, d. h. $G^{(\varrho+1)}(x_{\varrho+1} \dots x_n) \not\equiv 0\,(\mathfrak{o}_{\varrho\sigma})$, also auch $G^{(\varrho+1)}(x_{\varrho+1} \dots x_n) \not\equiv 0\,(\mathfrak{m}, \mathfrak{o}_{\varrho\sigma}^{\varkappa})$.

Es sei nun $g \equiv 0\,(\mathfrak{q}_{\varrho\sigma})$, dann gibt es ein $f^{(\varrho+1)} \neq 0$, so daß $f^{(\varrho+1)} g \equiv 0\,(\mathfrak{m}, \mathfrak{p}_{\varrho\sigma}^{\varkappa})$. Es wird also $f^{(\varrho+1)} \cdot g \equiv 0\,(\mathfrak{m}, \mathfrak{o}_{\varrho\sigma}^{\varkappa})$. Da nun aber alle Potenzen von $f^{(\varrho+1)}$ von $x_1 \dots x_\varrho$ unabhängig und somit nicht durch das Primärideal $(\mathfrak{m}, \mathfrak{o}_{\varrho\sigma}^{\varkappa})$ teilbar sind, so wird $g \equiv 0\,(\mathfrak{m}, \mathfrak{o}_{\varrho\sigma}^{\varkappa})$ und somit

$$\mathfrak{q}_{\varrho\sigma} \equiv 0\,(\mathfrak{m}, \mathfrak{o}_{\varrho\sigma}^{\varkappa}).$$

Es ist also

$$[\mathfrak{q}_{11} \dots \mathfrak{q}_{nm_n}] \equiv 0\,(\mathfrak{m}, \mathfrak{o}_{ij}^{\varkappa}),$$

wo $\mathfrak{v}_{ij}$ ein beliebiges zu $\mathfrak{m}$ gehörendes Nullstellenideal bedeutet. Nach Satz 5 ist also

$$[q_{11} \cdots q_{nm_n}] \equiv 0(\mathfrak{m}).$$

Andererseits ist

$$\mathfrak{m} \equiv 0(q_{\varrho\sigma}).$$

Daraus folgt

$$\mathfrak{m} \equiv 0([q_{11} \cdots q_{nm_n}]).$$

Es ist also

$$\mathfrak{m} = [q_{11} \cdots q_{nm_n}],$$

q. e. d.

Die isolierten Komponenten von $\mathfrak{m}$ ergeben sich jetzt durch Zusammenfassen von Primäridealen, die zu isolierten Gruppen unter den Primidealen gehören; dabei besteht eine isolierte Gruppe aus Primidealen, die zu $\mathfrak{m}$ gehören, und enthält mit irgendeinem zu $\mathfrak{m}$ gehörigen Primideal $\mathfrak{p}$ auch alle zu $\mathfrak{m}$ gehörigen Primideale, die Vielfache von $\mathfrak{p}$ sind. Da man nach Satz 3 mit endlich vielen Schritten feststellen kann, ob ein Ideal durch ein anderes teilbar ist, so kann man diese isolierten Gruppen mit endlich vielen Schritten berechnen. Dividiert man das Ideal $\mathfrak{m}$ durch das Produkt der $\varkappa$-ten Potenzen der Primideale der komplementären Gruppe, so erhält man ebenfalls die zugehörige isolierte Komponente, da ja $\varkappa$ nach Satz 12 eine obere Schranke für die Exponenten der auftretenden Primärideale ist.

(Eingegangen am 29. 5. 1925.)