

Werk

Titel: Eliminationstheorie und allgemeine Idealtheorie

Autor: Noether, E.

Jahr: 1923

PURL: https://resolver.sub.uni-goettingen.de/purl?235181684_0090|log25

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

✉ info@digizeitschriften.de

Eliminationstheorie und allgemeine Idealtheorie.

Von

Emmy Noether in Göttingen

Es handelt sich im folgenden um eine Einordnung der Eliminationstheorie — in der arithmetischen Fassung, die ich der Hentzeltschen Darstellung gegeben habe¹⁾ und die sich als eine Idealtheorie im Polynombereich bezeichnen läßt — in die allgemeine Idealtheorie²⁾, zugleich um eine Neubegründung der auf die Nullstellen bezüglichen Teile. Die Grundbegriffe beider Theorien sind in § 1 kurz zusammengestellt, ebenso die der Körpertheorie³⁾, so daß ich mich hier darauf beziehen kann.

Einordnung und Neubegründung gruppieren sich um vier Fragestellungen: Arithmetische Fassung des Dimensionsbegriffes; Theorie der Nullstellen; Zusammenhang der Zerlegungssätze für Normen und Elementarteiler mit denen der allgemeinen Idealtheorie; Charakterisierung der Primideale und Primärideale durch Norm und Elementarteilerform.

Die arithmetische Fassung des *Dimensionsbegriffes* (§ 4) geschieht durch Ketten von Primidealen, das arithmetische Äquivalent dafür, daß es auf Flächen Kurven, auf Kurven Punkte gibt. Diese arithmetische Fassung, die mit der Parameterdefinition der Eliminationstheorie als identisch nachgewiesen wird, läßt sich mit leichter Modifikation auf beliebige Ringbereiche übertragen und gibt dort zusammen mit der Übertragung gewisser Teile der übrigen Fragestellungen eine genaue Einsicht in den Aufbau der Ideale, wie ich an anderer Stelle zeigen werde.

Die Frage der *Nullstellen* wird bei H.-N. wie üblich für das gegebene Ideal direkt in Angriff genommen, und zwar durch Zurückgehen auf suk-

¹⁾ Hentzelt, Kurt: Zur Theorie der Polynomideale und Resultanten. Bearbeitet von E. Noether. Math. Ann. **88** (1922), S. 53—79; zitiert H.-N.

²⁾ Noether, E.: Idealtheorie in Ringbereichen, Math. Ann. **83** (1921), S. 24—66; zitiert Idealtheorie.

³⁾ Steinitz, E.: Algebraische Theorie der Körper, J. f. M. **137** (1910), S. 167—309; zitiert Steinitz.

zessive Elimination, wobei der Charakter des Verifizierens nicht ganz vermieden wird. Im Gegensatz dazu steht der für Polynome einer Veränderlichen stets begangene Weg; man stellt das gegebene Polynom als Produkt von Potenzen von Primfunktionen (Primärfunktionen) dar und konstruiert für jede einzelne Primfunktion den Nullstellenkörper als einen dem Restklassenkörper isomorphen Körper. Der Grad der Primfunktion gibt den Grad dieses Körpers; der Grad der Primärfunktion aber, deren Nullstellen mit denen der Primfunktion übereinstimmen, gibt den Grad des Ringes der Restklassen nach dieser Primärfunktion. Geht man bei jeder Primfunktion zum Galoisschen Körper über, so kommt die Zerlegung in Linearfaktoren; und damit ist für das ursprünglich gegebene Polynom die Frage der Nullstellen, Zerlegung in Linearfaktoren und Multiplizität erledigt. Ganz entsprechend wird hier (§ 3) das System der Restklassen nach einem Primideal durch Quotientenbildung zum Restklassenkörper erweitert und ein dazu isomorpher Nullstellenkörper konstruiert. Dieser Nullstellenkörper enthält einen durch Adjunktion von Unbestimmten — etwa $x_{i+1}, \dots, x_n$ — erzeugten Teilkörper; der Grad der Norm gibt den Grad in bezug auf diesen Teilkörper; zugleich ergibt sich durch Übergang zum Galoisschen Körper die Zerlegung der Elementarteilerform und damit der Norm in Linearfaktoren. Für das zugehörige Primärideal aber sind die Nullstellen die gleichen; die Zerlegung ist ebenfalls mitgegeben, da die Norm eine Potenz der Elementarteilerform des Primideals wird (§ 2); der Grad der Norm gibt den Grad des Ringes der Restklassen nach dem Primärideal in bezug auf den aus den Unbestimmten abgeleiteten Teilkörper.

Damit ist aber die Frage der Nullstellen eines beliebigen Ideals zurückgeführt auf den *Zusammenhang der Zerlegungssätze für Normen und Elementarteiler mit denen der allgemeinen Idealtheorie* (§ 5). Der Tatsache, daß die Nullstellen des Ideals sich aus denen seiner einzelnen zugehörigen Primideale zusammensetzen, entspricht die Zerlegung der Norm in größte primäre Faktoren, die gleich Potenzen der Elementarteilerform der einzelnen zugehörigen Primideale werden⁴⁾; damit ist die Zerlegung in Linearfaktoren für die Norm allgemein geleistet. Die Multiplizität aber findet bei H.-N. ihre Deutung vermöge der Grundideale und ihrer Komponenten; es wird der Grad eines größten primären Faktors der Norm gleich der Anzahl linear unabhängiger Restklassen — bei Adjunktion von $x_{i+1}, \dots, x_n$ — des Grundideals $(i-1)$ -ter Stufe nach einer Komponente des Grundideals i -ter Stufe. Nun wird das Grundideal $(i-1)$ -ter Stufe als

⁴⁾ Dieses Parallelgehen der Eliminationstheorie mit der allgemeinen Idealtheorie ist bei der Kroneckerschen Eliminationstheorie nicht erfüllt; vgl. dazu H.-N., Anm. 4).

identisch nachgewiesen mit der isolierten Komponente der Zerlegung, die eindeutig definiert ist durch alle Primideale von höherer als der $(n - i)$ -ten Dimension; eine Komponente des Grundideals i -ter Stufe aber als identisch mit der isolierten Komponente der Zerlegung, die definiert ist durch das dem Faktor der Norm entsprechende Primideal und alle Primideale höherer Dimension. Und der Grad des entsprechenden Faktors der Norm wird — bei Adjunktion von $x_{i+1}, \dots, x_n$ — gleich dem Grad desjenigen Teilringes der Restklassen dieser Komponente, der nur aus Klassen des Grundideals $(i - 1)$ -ter Stufe besteht.

Die *Charakterisierung der Primideale und eigentlichen Primär Ideale* (§ 6) ergibt sich als direkte Folgerung der Betrachtung der Restklassenkörper. Ist der ursprüngliche Koeffizientenbereich ein vollkommener Körper, so entsprechen den Primidealen als Norm und Elementarteilerform Primfunktionen, den eigentlichen Primär Idealen eigentliche Primärfunktionen, und umgekehrt. Bei unvollkommenem Körper als Koeffizientenbereich lassen sich nur Bedingungen angeben, die entweder notwendig oder hinreichend sind; es kann, wie an Beispielen gezeigt wird, die Norm eines Primideals eigentlich primär werden, die Elementarteilerform eines eigentlichen Primär Ideals eine Primfunktion. Genauer wird hier bei Charakteristik p die Norm eines Primideals die p^g -te Potenz ($g \geq 0$) seiner Elementarteilerform; während bei eigentlichen Primär Idealen, deren Elementarteilerform eine Primfunktion ist, die Norm eine beliebige Potenz werden kann, wie wieder Beispiele zeigen. Es werden schließlich noch *absolute Primideale* betrachtet (§ 7), d. h. solche, die Primideale bleiben bei Erweiterung des Koeffizientenbereiches zu einem algebraisch abgeschlossenen Körper. Bei absoluten Primidealen mit Koeffizienten aus einem (endlichen) algebraischen Zahlkörper führt die Charakterisierung zur Übertragung eines zuerst von A. Ostrowski für absolute Primfunktionen aufgestellten Satzes: Es bleibt die Eigenschaft, Primideal zu sein, erhalten modulo jedes Primideals des Zahlkörpers, höchstens mit endlich vielen Ausnahmen.

Es sei noch auf die Analogie der letzten Fragestellung mit der Idealtheorie in algebraischen Zahlkörpern hingewiesen. Als Elementarteilerform eines solchen Ideals ist die kleinste durch das Ideal teilbare ganze rationale Zahl aufzufassen (Anm. ¹⁰), die also für ein Primideal stets Primzahl wird, während umgekehrt ein Ideal Primideal wird, sobald seine Norm Primzahl ist; auch die Beweise laufen ganz parallel. Die oben angeführten Beispiele zeigen also, daß bei unvollkommenem Körper das Analogon zu Primidealen höheren Grades und zu Verzweigungsidealien auftritt, während es bei vollkommenem Körper nur Primideale ersten Grades und keine Verzweigungsidealien gibt.

§ 1.

**Grundbegriffe der Eliminationstheorie, allgemeinen Idealthorie
und Körpertheorie.**

1. Der Bereich. Es bezeichne $\bar{\mathfrak{S}}$ den Integritätsbereich aller Polynome in $y_1, \dots, y_n$ mit Koeffizienten aus einem abstrakt definierten Körper P . Die y seien einer Transformation mit Unbestimmten $u_{\mu\nu}$ als Koeffizienten unterworfen⁵⁾:

$$(1) \quad y_1 = u_{11}x_1 + \dots + u_{1n}x_n; \dots; y_n = u_{n1}x_1 + \dots + u_{nn}x_n$$

mit der Umkehrung

$$(1') \quad x_1 = t_{11}y_1 + \dots + t_{1n}y_n; \dots; x_n = t_{n1}y_1 + \dots + t_{nn}y_n,$$

und die $u_{\mu\nu}$ oder — was wegen der gegenseitig rationalen Ausdrückbarkeit damit gleichbedeutend ist — die $t_{\mu\nu}$ zu P adjungiert, so daß der Koeffizientenbereich $P(u) = P(t)$ entsteht; $\mathfrak{S}$ bezeichne den Integritätsbereich aller Polynome in $x_1, \dots, x_n$ mit Koeffizienten aus $P(u)$. Die Bereiche $\mathfrak{S}$ und $\bar{\mathfrak{S}}$ liegen der Eliminationstheorie zugrunde; es werden Ideale $\mathfrak{a}, \mathfrak{b}, \dots$ in $\mathfrak{S}$ und $\bar{\mathfrak{a}}, \bar{\mathfrak{b}}, \dots$ in $\bar{\mathfrak{S}}$ betrachtet. Ein Ideal in einem beliebigen Ring ist dabei wie üblich dadurch definiert, daß es neben α und β auch $\alpha - \beta$ enthält, neben α auch $\lambda\alpha$, unter λ ein beliebiges Ringelement verstanden; $\mathfrak{o}$ bedeute stets das aus allen Elementen bestehende Einheitsideal.

2. Transformierte Ideale. Ein Ideal $\mathfrak{m}$ in $\mathfrak{S}$ heißt transformiert, wenn es aus einem Ideal $\bar{\mathfrak{m}}$ in $\bar{\mathfrak{S}}$ vermöge (1) bei Adjunktion der $u_{\mu\nu}$ oder $t_{\mu\nu}$ entsteht. $\mathfrak{m}$ besteht also, wenn $\bar{f}(y)$ oder $\bar{g}(y)$ alle Polynome aus $\bar{\mathfrak{m}}$ durchlaufen, aus allen linearen Verbindungen

$$f(x) = \sum U_i(u) \bar{f}_i(y) = \sum U_i(u) f_i(x)$$

oder auch

$$g(x) = \sum T_i(t) \bar{g}_i(y) = \sum T_i(t) g_i(x);$$

hierin sind insbesondere alle $f_i(x) = \bar{f}_i(y)$ enthalten, oder, was auf dasselbe hinauskommt, alle $g_i(x) = \bar{g}_i(y)$. Da $f(x)$ bzw. $g(x)$ nur bis auf Größen aus $P(u) = P(t)$ festgelegt sind, dürfen die U_i, T_i ohne Beschränkung der Allgemeinheit als Potenzprodukte der u bzw. t angenommen werden. $f(x), g(x)$ gehen wieder in Polynome aus $\mathfrak{m}$ über, wenn U, T durch irgendwelche anderen Potenzprodukte ersetzt werden, also insbesondere durch Vertauschen der Spalten von (1) bzw. der Zeilen von (1'); somit enthält $\mathfrak{m}$ neben irgendeinem Polynom auch alle durch Vertauschung der x

⁵⁾ Die Transformation ist im Hinblick auf § 3 usw. etwas allgemeiner als bei H.-N., wodurch alle dortigen Resultate um so mehr erhalten bleiben.

daraus entstehenden, sofern nur in den von u bzw. t abhängenden Koeffizienten die entsprechenden Vertauschungen vorgenommen werden. Alle im folgenden auftretenden Ideale sollen — wenn nicht ausdrücklich das Gegenteil bemerkt ist — als transformiert angenommen werden. Nichttransformierte Ideale gehen durch Zusammensetzen von (1) mit $x_i = v_{i1}z_1 + \dots + v_{in}z_n$ in transformierte im Polynombereich der z mit Koeffizienten aus $P(u, v)$ über, während dieses Zusammensetzen bei transformierten Idealen nur auf ein Ersetzen der $u_{\mu\nu}$ durch bilineare Verbindungen der u, v herauskommt.

3. Bezeichnung. Unter $f^{(i)}, g^{(i)}, \dots, a^{(i)}, b^{(i)}, \dots$ seien durchweg Polynome in $\mathfrak{S}$ verstanden, die von $x_1, \dots, x_{i-1}$ frei sind.

4. Grundideale. Jedem Ideal m sind n Grundideale $g_0, g_1, \dots, g_{n-1}$ zugeordnet durch die Festsetzung: Das Grundideal $(i-1)$ -ter Stufe g_{i-1} enthält alle und nur die Polynome $G(x)$, für die es ein — im allgemeinen mit $G(x)$ sich änderndes — Polynom $b^{(i)} \neq 0$ gibt, derart, daß $b^{(i)}G(x) \equiv 0(m)$ wird. Aus der Existenz der Idealbasis folgt daraus auch die Existenz mindestens eines für alle $G(x)$ festen $B^{(i)}$, so daß also

$$(2) \quad B^{(i)}g_{i-1} \equiv 0(m), \quad B^{(i)} \neq 0$$

wird. Die Grundideale transformierter Ideale werden selbst transformierte Ideale (H.-N. Satz VI). Das Grundideal i -ter Stufe g_i ist auch definiert als das Ideal, in das m bei Adjunktion von $x_{i+1}, \dots, x_n$ zu $P(u)$ übergeht, wenn man sich — was dann keine Beschränkung der Allgemeinheit bedeutet — auf in $x_{i+1}, \dots, x_n$ ganze Polynome beschränkt; g_0 wird stets gleich dem Einheitsideal $\mathfrak{o}$.

5. Modularstellung der Ideale, Elementarteiler und Einzelnormen. Faßt man jedes Polynom $f(x)$ auf als Linearform in den Potenzprodukten ξ von $x_1, \dots, x_{i-1}$, mit Polynomen $a^{(i)}$ als Koeffizienten, so geht das Ideal m über in einen Modul $\mathfrak{M}_{i-1}$ aus Linearformen in bezug auf den Bereich der $a^{(i)}$; d. h. $\mathfrak{M}_{i-1}$ enthält neben irgend zwei Linearformen auch ihre Differenz, neben einer Linearform $l(\xi)$ auch $a^{(i)}l(\xi)$ bei beliebigem $a^{(i)}$. Als Grundmodul eines solchen Moduls $\mathfrak{M}$ wird die Gesamtheit der Linearformen $g(\xi)$ bezeichnet, für die $b^{(i)}g(\xi) \equiv 0(\mathfrak{M})$, $b^{(i)} \neq 0$ wird; das Grundideal g_{i-1} geht also bei der Modularstellung in den Grundmodul $\mathfrak{G}_{i-1}$ von $\mathfrak{M}_{i-1}$ über. $\mathfrak{M}_{i-1}$ und $\mathfrak{G}_{i-1}$ hängen von unendlich vielen Unbestimmten ξ ab, derart, daß in jeder einzelnen Linearform nur endlich viele dieser Unbestimmten auftreten. $\mathfrak{M}_{i-1}$ hat die charakteristische Eigenschaft, bei Adjunktion von $x_{i+1}, \dots, x_n$ zu $P(u)$ nur endlich viele von der Einheit verschiedene Elementarteiler zu besitzen; d. h. $\mathfrak{G}_{i-1}$ und $\mathfrak{M}_{i-1}$ lassen bei dieser Adjunktion eine Basisdarstellung zu — unter ζ neue Unbestimmte verstanden, die mit den ξ durch umkehrbar lineare, in x_i

ganze Transformation zusammenhängen, derart, daß in $\zeta_i = r_i(\xi)$, $\xi_k = s_k(\zeta)$ nur jeweils endlich viele dieser Unbestimmten auftreten —

$$(3) \quad \begin{aligned} \mathfrak{G}_{i-1} &= (\zeta_0, \zeta_1, \dots, \zeta_\sigma, \zeta_{\sigma+1}, \dots, \zeta_{\sigma+r}, \dots); \\ \mathfrak{M}_{i-1} &= (E^{(i)}\zeta_0, E^{(i)}\zeta_1, \dots, E^{(i)}\zeta_\sigma, \zeta_{\sigma+1}, \dots, \zeta_{\sigma+r}, \dots), \end{aligned}$$

wo jedes $E^{(i)}_\mu$ im vorangehenden aufgeht (H.-N. (24) und (28)).

Der *höchste Elementarteiler* $E^{(i)}$ ist auch definiert als größter gemeinsamer Teiler — im Polynomsinn — aller in (2) auftretenden $B^{(i)}$; er kann als ganz und primitiv in $x_{i+1}, \dots, x_n$ angenommen werden und wird dann regulär in x_i , d. h. $E^{(i)}$ enthält den Term x_i^λ mit von Null verschiedenem Koeffizienten, wenn es vom Grade λ in den x ist.

Das Produkt $R^{(i)}$ aller in (3) auftretenden Elementarteiler wird als Norm von $\mathfrak{G}_{i-1}$ nach $\mathfrak{M}_{i-1}$ oder auch als *Einzelnorm* des Ideals $\mathfrak{m}$ bezeichnet; in Zeichen und unter Berücksichtigung, daß $\mathfrak{m}$ bei der Adjunktion von $x_{i+1}, \dots, x_n$ in $\mathfrak{g}_i$ übergeht:

$$R^{(i)} = E^{(i)} E_1^{(i)} \dots E_\sigma^{(i)} = N(\mathfrak{G}_{i-1} | \mathfrak{M}_{i-1}) = N(\mathfrak{g}_{i-1} | \mathfrak{g}_i).$$

Wie (3) zeigt, wird $R^{(i)}$ bei Adjunktion von $x_{i+1}, \dots, x_n$ gleich der Determinante der Übergangssubstitution von $\mathfrak{G}_{i-1}$ nach $\mathfrak{M}_{i-1}$, und der Grad von $R^{(i)}$ gibt die Anzahl der in bezug auf $P(u, x_{i+1}, \dots, x_n)$ linear unabhängigen Restklassen von $\mathfrak{G}_{i-1}$ nach $\mathfrak{M}_{i-1}$, also von $\mathfrak{g}_{i-1}$ nach $\mathfrak{g}_i$ an; $R^{(i)}$ kann als ganz und primitiv in $x_{i+1}, \dots, x_n$ angenommen werden und wird dann regulär in x_i . $R^{(i)}$ läßt sich berechnen als größter gemeinsamer Teiler — im Polynomsinn — aller ϱ -reihigen Determinanten irgendeines stets existierenden Moduls $\mathfrak{M}_{i-1}^*$ vom Range ϱ von der Eigenschaft, daß das Restklassensystem $\mathfrak{G}_{i-1}^* | \mathfrak{M}_{i-1}^*$ isomorph wird zu $\mathfrak{G}_{i-1} | \mathfrak{M}_{i-1}$, unter $\mathfrak{G}_{i-1}^*$ den Grundmodul von $\mathfrak{M}_{i-1}^*$ verstanden (H.-N. Satz VII und § 5).

6. Elementarteilerform und Norm (Resultantenform) der Ideale. Das Produkt $E_{\mathfrak{m}} = E^{(1)} E^{(2)} \dots E^{(n)}$ aller höchsten Elementarteiler wird als *Elementarteilerform*, das Produkt $R_{\mathfrak{m}} = R^{(1)} R^{(2)} \dots R^{(n)}$ aller Einzelnormen als *Norm* (Resultantenform)⁶⁾ von $\mathfrak{m}$ bezeichnet. Elementarteilerform und Norm werden durch das Ideal teilbar; die Norm wird durch die Elementarteilerform, eine Potenz der letzteren durch die Norm teilbar. Allgemeiner gilt noch:

$$(4) \quad \begin{aligned} E^{(i)} \mathfrak{g}_{i-1} &\equiv 0(\mathfrak{g}_i); \quad E^{(n)} \dots E^{(i)} \mathfrak{g}_{i-1} \equiv 0(\mathfrak{m}) \quad \text{und folglich} \\ R^{(i)} \mathfrak{g}_{i-1} &\equiv 0(\mathfrak{g}_i); \quad R^{(n)} \dots R^{(i)} \mathfrak{g}_{i-1} \equiv 0(\mathfrak{m}), \quad (\text{H.-N. Satz VIII}), \end{aligned}$$

und weiter: Ist $\mathfrak{m}$ teilbar durch $\mathfrak{n}$, und stimmen die Normen $R_{\mathfrak{m}}$ und $R_{\mathfrak{n}}$

⁶⁾ Bei H.-N. wird nur die Bezeichnung Resultantenform gebraucht; die Bezeichnung Norm entspricht den arithmetischen Eigenschaften.

überein, so stimmen auch die Ideale m und n überein (H.-N. Satz IX). Beachtet man, daß für einen Teiler von m aus dem Übereinstimmen von $R^{(1)}, R^{(2)} \dots$ das Übereinstimmen der Grundideale $g_1, g_2 \dots$ folgt und daß stets $g_0 = 0$ ist, so kommt ganz entsprechend: Ist n ein echter Teiler von m , so wird die erste Einzelnorm von n , die von der entsprechenden von m verschieden ist, ein echter Teiler⁷⁾. Enthält m ein Polynom $G^{(i)} \neq 0$, so werden nach Definition $g_0, g_1, \dots, g_{i-1}$ gleich dem Einheitsideal; und somit werden $R^{(1)}, \dots, R^{(i-1)}$ nach der in 5. angegebenen Eigenschaft der Einzelnormen, die Anzahl linear unabhängiger Restklassen zu bestimmen, gleich der Einheit; folglich werden auch $E^{(1)}, \dots, E^{(i-1)}$ gleich der Einheit.

7. Zerlegung der Einzelnormen und Elementarteiler; Komponenten der Grundideale. Unter einer Primfunktion wird ein in bezug auf $P(u)$ irreduzibles Polynom verstanden, unter Primärfunktion die Potenz einer Primfunktion; eine eigentliche Primärfunktion ist eine solche, die nicht zugleich Primfunktion ist, wo es sich also um höhere als erste Potenz handelt. Eine Zerlegung eines Polynoms in größte primäre Faktoren ist eine solche, wo jeder Faktor Primärfunktion ist, das Produkt irgend zweier Faktoren aber nicht mehr primär⁸⁾. Der Zerlegung der Einzelnorm $R^{(i)} = N(g_{i-1} | g_i)$ in größte primäre Faktoren $Q_\lambda^{(i)}$ entspricht eine Darstellung von g_i als kleinstes gemeinsames Vielfaches $g_i = [r_1, r_2, \dots, r_a]$, derart, daß $Q_\lambda^{(i)} = N(g_{i-1} | r_\lambda)$ wird; r_λ besitzt dabei g_{i-1} als Grundideal $(i-1)$ -ter Stufe, und stimmt mit seinem Grundideal i -ter Stufe überein; die r_λ werden als die Komponenten der Grundideale bezeichnet. Der höchste Elementarteiler von r_λ wird gleich dem größten gemeinsamen Teiler — im Polynomsinn — von $Q_\lambda^{(i)}$ und $E^{(i)}$, also gleich einem größten primären Faktor von $E^{(i)}$. Die r_λ sind eindeutig bestimmt durch ihr oben angegebenes Verhalten in bezug auf die Grundideale und durch die Forderung, daß entweder Einzelnorm oder höchster Elementarteiler ein größter primärer Faktor von $R^{(i)}$ bzw. $E^{(i)}$ werden soll (H.-N. Satz X).

8. Dimensionsbegriff. Dem Ideal m wird die Höchstdimension $n - i$ zugeschrieben, wenn $R^{(i)}$ die erste von der Einheit verschiedene Einzelnorm ist — oder was nach 6. damit gleichbedeutend ist, wenn g_i das erste vom Einheitsideal verschiedene Grundideal ist; dem Einheits-

⁷⁾ Dagegen können spätere Faktoren von R_m Vielfache der entsprechenden Faktoren von R_n werden; z. B. immer, wenn m Primideal ist und n nicht das Einheitsideal.

⁸⁾ Die Definition von Primfunktion und Primärfunktion ließe sich auch in genauer Analogie mit 11. fassen, indem man nur das Wort Ideal durch Polynom ersetzt. Die größten primären Faktoren sind das Analogon zu den größten primären Komponenten der Zerlegung in 12.

ideal $\mathfrak{o}$ wird die Dimension -1 zugeschrieben. Ist nur *eine* von der Einheit verschiedene Einzelnorm $R^{(i)}$ vorhanden, wird also $\mathfrak{g}_i = \mathfrak{g}_{i+1} = \dots = \mathfrak{m}$, so wird die Höchstdimension auch als Dimension von $\mathfrak{m}$ bezeichnet. Enthält $\mathfrak{m}$ ein Polynom $G^{(i)} \neq 0$, so ist es höchstens von der Höchstdimension $n-i$, wie die Bemerkung am Schluß von 6. zeigt. Ist $\mathfrak{m}$ von der Höchstdimension $n-i$, $\mathfrak{n}$ ein Teiler $\mathfrak{m}$, so ist $\mathfrak{n}$ also höchstens von der Höchstdimension $n-i$.

9. Norm (Resultantenform) und Nullstellen. Unter Nullstellen eines Ideals $\mathfrak{m}$ werden alle einem geeigneten algebraischen Erweiterungskörper von $P(u; x_{i-1}, \dots, x_n)$ angehörigen Wertsysteme von $x_1, \dots, x_i$ verstanden ($i=1, 2, \dots, n$), für welche — unter Adjunktion von $x_{i+1}, \dots, x_n$ zum Koeffizientenbereich — alle Polynome aus $\mathfrak{m}$ verschwinden. Jedem Faktor $R^{(i)}$ der Norm (Resultantenform) entsprechen bei dieser Adjunktion so viele Nullstellen von $\mathfrak{m}$, wie der Grad von $R^{(i)}$ angibt; und es läßt $R^{(i)}$, geschrieben in bilinearen Verbindungen w_u , der u_{uv} und weiterer Unbestimmten v , die explizite Zerlegung zu:

$$R^{(i)} = \prod \{z - (v_1 \bar{x}_{1,r} + \dots + v_{i-1} \bar{x}_{i-1,r} + v_i \bar{x}_{i,r})\}^r,$$

wo $\bar{x}_{1,r}, \dots, \bar{x}_{i,r}$ ein System zusammengehöriger Nullstellen bedeutet (H.-N. Satz XIII; eine neue Begründung wird in § 3 gegeben werden). Unter den Nullstellen eines Ideals von der Höchstdimension $n-i$ gibt es also solche, die von $(n-i)$ Parametern abhängen, aber keine die von mehr Parametern abhängen; damit ist aber die Übereinstimmung des unter 8. gegebenen Dimensionsbegriffs mit der gewöhnlich üblichen Fassung gezeigt.

10. Der Ringbereich der allgemeinen Idealtheorie. Der zugrunde gelegte Bereich sei ein kommutativer Ring, in dem der Satz von der endlichen Kette gilt: Jede Kette von Idealen $\mathfrak{a}, \mathfrak{a}_1, \dots, \mathfrak{a}_r, \dots$, wo jedes $\mathfrak{a}_i$ ein echter Teiler — Teiler im Idealsinn — des unmittelbar vorangehenden ist, bricht im Endlichen ab. Diese Forderung ist äquivalent mit der anderen, daß jedes Ideal eine Idealbasis besitzt (Idealtheorie, Satz I), ist also insbesondere für den Polynombereich erfüllt. In den folgenden Nummern 11., 12., 13. wird dieser allgemeine Ringbereich zugrunde gelegt.

11. Primideale und Primär ideale. Ein Ideal $\mathfrak{p}$ heißt Primideal, wenn aus der Teilbarkeit eines Produktes durch $\mathfrak{p}$ die Teilbarkeit mindestens eines Faktors folgt; $\mathfrak{q}$ heißt Primär ideal — oder primär —, wenn aus der Teilbarkeit eines Produktes durch $\mathfrak{q}$ die Teilbarkeit eines Faktors oder einer Potenz jedes Faktors folgt. In Zeichen:

$$\text{aus } \mathfrak{a} \equiv 0(\mathfrak{p}), \quad \mathfrak{b} \equiv 0(\mathfrak{p}) \text{ folgt } \mathfrak{ab} \equiv 0(\mathfrak{p});$$

$$\text{aus } \mathfrak{a} \equiv 0(\mathfrak{q}), \quad \mathfrak{b}^x \equiv 0(\mathfrak{q}) \text{ für jede Potenz } x \text{ folgt } \mathfrak{ab} \equiv 0(\mathfrak{q}).$$

Zu jedem Primärideal q gibt es ein und nur ein zugehöriges Primideal p , das Teiler von q ist und von dem eine Potenz durch q teilbar wird, $q \equiv 0(p)$; $p^e \equiv 0(q)$; dabei besteht p aus allen Ringelementen, von denen eine Potenz durch q teilbar wird. Wie die Definition zeigt, ist jedes Primideal zugleich Primärideal; unter eigentlichen Primäridealien werden solche verstanden, die nicht zugleich Primideal sind, für die also $q > 1$ wird.

12. Der Zerlegungssatz. Eine Darstellung $a = [q_1, \dots, q_\alpha]$ eines Ideals als kleinstes gemeinsames Vielfaches heißt eine kürzeste, wenn kein q im kleinsten gemeinsamen Vielfachen der übrigen — in seinem Komplement — aufgeht; sie heißt eine solche durch größte primäre Komponenten, wenn jedes q primär ist, aber das kleinste gemeinsame Vielfache irgend zweier q nichtprimär ist. Jedes Ideal läßt eine kürzeste Darstellung durch endlich viele größte primäre Komponenten zu; bei zwei verschiedenen solchen Darstellungen stimmen die Anzahl der Komponenten und die zugehörigen Primideale, die alle voneinander verschieden sind, überein. Die derart eindeutig bestimmten Primideale sollen als die Primideale oder zugehörigen Primideale des Ideals bezeichnet werden (Idealtheorie, Satz IX).

13. Isolierte Komponenten der Zerlegung. Ein Ideal $r = [q_{i_1}, \dots, q_{i_r}]$ wird isolierte Komponente der Zerlegung von a genannt, wenn die q_{i_λ} in mindestens einer kürzesten Darstellung von a durch größte primäre Komponenten auftreten und die Bedingung erfüllen, daß keines ihrer zugehörigen Primideale in einem der übrigen Primideale von a aufgeht. Die isolierten Komponenten der Zerlegung sind eindeutig durch ihre Primideale bestimmt; insbesondere sind also die isolierten größten primären Komponenten eindeutig bestimmt (Idealtheorie, Satz XIII).

14. Charakteristik, vollkommene und unvollkommene Körper, Erweiterung erster Art. Ein Körper Ω heißt von der Charakteristik Null, wenn der in Ω enthaltene, aus der Einheit abgeleitete Primkörper vom Typus des Körpers der rationalen Zahlen ist; von der Charakteristik p , wenn dieser Primkörper vom Typus des Restklassensystems nach einer Primzahl p ist. Ein Körper Ω heißt vollkommen, wenn jede Primfunktion mit Koeffizienten aus Ω in einem geeigneten Erweiterungskörper in getrennte Linearfaktoren zerfällt, im entgegengesetzten Falle unvollkommen. Jeder Körper von der Charakteristik Null ist vollkommen; ein Körper von der Charakteristik p aber dann und nur dann, wenn er neben jedem Element auch dessen p -te Wurzel enthält. Eine Primfunktion in einem unvollkommenen Körper ist eine ganze Funktion r -ten Grades von x^{p^f} , und zerfällt in einem geeigneten Erweiterungskörper in p^f -te Potenzen von r verschiedenen Linearfaktoren; f wird als Exponent bezeichnet. Eine Primfunktion heißt von erster Art, wenn sie

in einem geeigneten Erweiterungskörper in getrennte Linearfaktoren zerfällt, der Exponent f Null wird; eine Erweiterung heißt erster Art, wenn jedes Element erster Art, d. h. Nullstelle einer Primfunktion erster Art wird. Jede Erweiterung, die durch Adjunktion eines Elementes erster Art entsteht, ist erster Art; bei vollkommenen Körpern gibt es nur Erweiterungen erster Art (Steinitz, § 11 und § 13).

15. Reduzierter Grad und Exponent einer endlichen Erweiterung. Ist $\mathfrak{L}$ eine endliche Erweiterung eines unvollkommenen Körpers Ω , so ist in $\mathfrak{L}$ ein Teilkörper $\mathfrak{L}_0$ vom Grade r enthalten, der erster Art in bezug auf Ω wird und der aus allen und nur den Elementen erster Art aus $\mathfrak{L}$ besteht. Die p^f -te Potenz jedes Elementes aus $\mathfrak{L}$ gehört zu $\mathfrak{L}_0$, und es gibt Elemente in $\mathfrak{L}$, die genau vom Grade rp^f sind. r wird als reduzierter Grad, f als Exponent der endlichen Erweiterung bezeichnet (Steinitz, § 14, 1 und § 14, 5).

§ 2.

Elementarteilerform und Norm der Primideale und Primär Ideale. Teiler der Primideale.

Es handelt sich von jetzt an durchweg um den in § 1, 1. definierten Polynombereich. Vorerst ist zu zeigen, daß man sich auch bei Primidealen und Primär Idealen auf transformierte Ideale beschränken kann, nach

Hilfssatz I. *Das transformierte Ideal $\mathfrak{p}$ eines Primideals $\bar{\mathfrak{p}}$ in $\bar{\mathfrak{S}}$ wird Primideal, das transformierte $\mathfrak{q}$ eines Primär Ideals $\bar{\mathfrak{q}}$ in $\bar{\mathfrak{S}}$ wird Primärideal. M. a. W. die Eigenschaft, Primideal oder Primärideal zu sein, bleibt bei Adjunktion der u_{μ} zu P erhalten.*

Sei nämlich vorausgesetzt: $a \not\equiv 0(\mathfrak{p})$, $b \not\equiv 0(\mathfrak{p})$, wo a und b nicht notwendig transformierte Ideale zu sein brauchen; sei etwa $a(x) \equiv 0(\mathfrak{p})$, $b(x) \not\equiv 0(\mathfrak{p})$, wo $a(x)$ und $b(x)$ Polynome aus a und b bedeuten. Durch Umkehrung von (1) nach (1') kommt — unter T ohne Beschränkung der Allgemeinheit Potenzprodukte der T_{μ} verstanden —

$$a(x) = \sum T_j \bar{a}_j(y); \quad b(x) = \sum T_j \bar{b}_j(y),$$

und es muß mindestens ein $\bar{a}_j(y)$ und ein $\bar{b}_j(y)$ nicht durch $\bar{\mathfrak{p}}$ teilbar sein. Seien etwa $\bar{a}_r(y) \not\equiv 0(\bar{\mathfrak{p}})$; $\bar{b}_s(y) \not\equiv 0(\bar{\mathfrak{p}})$ die jeweils höchsten Glieder bei irgendeiner lexikographischen Anordnung der T ; dann wird auch $\bar{a}_r(y) \bar{b}_s(y) \not\equiv 0(\bar{\mathfrak{p}})$ und somit kommt $a(x) b(x) \not\equiv 0(\mathfrak{p})$ und also $a b \not\equiv 0(\mathfrak{p})$, womit $\mathfrak{p}$ als Primideal nachgewiesen ist. Der Beweis beruht offenbar darauf, daß das System der Restklassen nach einem Primideal einen Ring

ohne Nullteiler bildet, eine Eigenschaft, die bei Adjunktion von Unbestimmten erhalten bleibt.

Sei entsprechend $a \not\equiv 0(q)$, $b^z \not\equiv 0(q)$ für jede Potenz z ; dann folgt aus der Existenz der Idealbasis, daß wieder ein $a(x)$ aus a und ein $b(x)$ aus b existieren muß, so daß $a(x) \not\equiv 0(q)$, $b(x)^z \not\equiv 0(q)$ für jede Potenz z wird; denn bei der entgegengesetzten Annahme würde eine Potenz von b durch q teilbar.

Setzt man $a(x)b(x) = c(x)$, so mögen a^* , b^* , c^* die bzw. aus den Koeffizienten $\bar{a}_j(y)$, $\bar{b}_j(y)$, $\bar{c}_j(y)$ von $a(x)$, $b(x)$, $c(x)$ abgeleiteten Ideale bedeuten. Dann wird $b^{*z} \equiv 0(\bar{q})$ für jede Potenz z , da sonst $b(x)^z$ durch q teilbar würde; wegen $a^* \equiv 0(\bar{q})$ muß daher auch $a^* b^{*z} \equiv 0(\bar{q})$ für jede Potenz z werden. Nun existiert aber nach dem Dedekind-Mertensschen Satze⁹⁾ ein Exponent h derart, daß $a^* b^{*h} = b^{*h-1} c^*$ wird; also muß $c^* \equiv 0(\bar{q})$ werden. Das ergibt aber $c(x) \equiv 0(q)$ und somit $ab \equiv 0(q)$, womit q als primär nachgewiesen ist.

Auch bei der Darstellung eines Ideals als kleinstes gemeinsames Vielfaches kann man sich auf transformierte Ideale beschränken, nach

Hilfssatz II. *Aus einer Darstellung $\bar{m} = [\bar{c}_1, \dots, \bar{c}_a]$ in $\bar{\mathfrak{S}}$ folgt eine Darstellung $m = [c_1, \dots, c_a]$ in $\mathfrak{S}$, wo c_i die transformierten von $\bar{c}_i$ bedeuten. Insbesondere können also in jeder kürzesten Darstellung durch größte primäre Komponenten (§ 1, 12.) diese als transformiert angenommen werden.*

Es wird nämlich m durch $[c_1, \dots, c_a]$ teilbar, da jedes Polynom $f(x)$ aus m — eventuell nach Multiplikation mit einer geeigneten Potenz von u_{a^*} , — von der Form $\sum U_i \bar{f}_i(y)$ ist, wo jedes $\bar{f}_i(y)$ als Polynom aus $\bar{m}$ nach Voraussetzung durch alle $\bar{c}_i$ teilbar ist. Ist umgekehrt $f(x)$ durch jedes c_i teilbar, so wird es von obiger Form, und somit durch m teilbar. Geht man also von einer Zerlegung in größte primäre Komponenten in $\bar{\mathfrak{S}}$ aus, so ergibt dies eine Zerlegung $m = [q_1, \dots, q_a]$ in $\mathfrak{S}$; hier sind die q als transformierte von primären Idealen nach Hilfssatz I primär, und zwar handelt es sich um größte primäre Komponenten, da verschiedenen zugehörigen Primidealen $\bar{p}$ in $\bar{\mathfrak{S}}$ auch verschiedene p in $\mathfrak{S}$ entsprechen.

Es handelt sich jetzt um eine erste Charakterisierung von Primidealen und Primäridealien durch Elementarteilerform und Norm, noch ohne vollständige Trennung von prim und primär, und zwar gilt in genauer Analogie zu der Idealthorie in algebraischen Zahlkörpern¹⁰⁾

⁹⁾ Vgl. H.-N., S. 63 und Anm. ¹³⁾.

¹⁰⁾ Als höchsten Elementarteiler der Ideale in algebraischen Zahlkörpern hat man die kleinste durch das Ideal teilbare ganze rationale Zahl aufzufassen, also insbesondere die durch ein Primideal teilbare Primzahl oder die durch ein Primärideal

Satz I. Die Elementarteilerform eines Primideals wird gleich einer Primfunktion, die Norm gleich einer Potenz dieser Primfunktion. Bei Primäridealen werden Elementarteilerform und Norm gleich Primärfunktionen, und zwar gleich Potenzen derselben Primfunktion, die selbst Elementarteilerform des zugehörigen Primideals ist. Bei Primidealen und Primäridealen fällt die Höchstdimension mit der Dimension schlechthin zusammen; diese Dimension stimmt für Primärideal und zugehöriges Primideal überein.

Satz I ist offenbar erfüllt für das Einheitsideal, dessen Elementarteilerform und Norm gleich der Einheit werden. Sei jetzt das Primideal $\mathfrak{p}$ von der Höchstdimension $(n - i)$; nach (4), § 1, 6. kommt

$$E^{(n)} \dots E^{(i+1)} \mathfrak{g}_i \equiv 0(\mathfrak{p}); \quad \text{aber} \quad E^{(n)} \dots E^{(i+1)} \not\equiv 0(\mathfrak{p}),$$

da $\mathfrak{p}$ sonst nach § 1, 8. höchstens von der Höchstdimension $n - i - 1$ würde. Somit wird $\mathfrak{g}_i \equiv 0(\mathfrak{p})$, also $\mathfrak{p}$ mit seinem Grundideal i -ter Stufe und folglich auch mit $\mathfrak{g}_{i+1}, \mathfrak{g}_{i+2} \dots$ identisch. Es werden also $R^{(i+1)} = N(\mathfrak{g}_i, \mathfrak{g}_{i+1}), R^{(i+2)} \dots$ gleich der Einheit, mithin auch $E^{(i+1)}, E^{(i+2)} \dots$ als Teiler von $R^{(i+1)}, R^{(i+2)} \dots$; und somit wird die Elementarteilerform gleich $E^{(i)}$, das gleich einer Primfunktion $P^{(i)}$ werden muß. Denn nach § 1, 5. und unter Berücksichtigung, daß $\mathfrak{g}_{i-1}$ gleich dem Einheitsideal wird, ist $E^{(i)}$ definiert als größter gemeinsamer Teiler — im Polynomsinn — aller durch $\mathfrak{p}$ teilbaren $B^{(i)}$; aus $E^{(i)} = C_1^{(i)} C_2^{(i)} \equiv 0(\mathfrak{p})$ würde also folgen, daß $E^{(i)}$ in einem seiner Faktoren $C_1^{(i)}$ oder $C_2^{(i)}$ aufgehen muß. Da aber eine Potenz von $E^{(i)}$ durch $R^{(i)}$ teilbar wird, wird $R^{(i)}$ gleich einer Potenz — die auch die erste sein kann — dieser Primfunktion $P^{(i)}$; zugleich wird $R^{(i)}$ Norm von $\mathfrak{p}$. Da nur eine von der Einheit verschiedene Einzelnorm $R^{(i)}$ auftritt, stimmt schließlich die Höchstdimension von $\mathfrak{p}$ mit der Dimension schlechthin überein.

Sei entsprechend das Primärideal $\mathfrak{q}$ von der Höchstdimension $n - i$; dann kommt wie oben

$$E^{(n)} \dots E^{(i+1)} \mathfrak{g}_i \equiv 0(\mathfrak{q}); \quad (E^{(n)} \dots E^{(i+1)})^z \not\equiv 0(\mathfrak{q})$$

für jede Potenz z ; und folglich wird wie oben $\mathfrak{q} = \mathfrak{g}_i$, seine Elementarteilerform gleich $E^{(i)}$, seine Norm gleich $R^{(i)}$, die Höchstdimension gleich der Dimension schlechthin. Diese Dimension stimmt mit der des zugehörigen Primideals überein; denn aus $\mathfrak{p}^z \equiv 0(\mathfrak{q}); \mathfrak{q} \equiv 0(\mathfrak{p})$ folgt, daß

(Primidealpotenz) teilbare Primzahlpotenz. In der Tat ist ja jedes Ideal $\mathfrak{a}^*$ zugleich ein Modul $\mathfrak{A}^*$ aus Linearformen in den Elementen $\omega_1, \dots, \omega_n$ einer Körperbasis, $(\omega_1, \dots, \omega_n)$ Grundmodul von $\mathfrak{A}^*$; die kleinste durch $\mathfrak{a}^*$ teilbare ganze rationale Zahl wird also der höchste Elementarteiler dieses Moduls $\mathfrak{A}^*$; die Norm von $\mathfrak{a}^*$ aber wird das Produkt aller Elementarteiler von $\mathfrak{A}^*$.

die Dimension $(n - i)$ von p höchstens gleich der von q , die von q höchstens gleich der von p^e ist; aus $(P^{(i)})^e \equiv 0(p^e)$, wo $P^{(i)}$ die Elementarteilerform von p bedeutet, ergibt sich letztere Höchstdimension als höchstens $n - i$, und somit wird $n - i$ die Dimension von p und q . Aus $(P^{(i)})^e \equiv 0(q)$ folgt ferner, daß $E^{(i)}$ — als größter gemeinsamer Teiler aller $B^{(i)}$ aus q — eine Potenz von $P^{(i)}$ wird, die auch die erste sein kann, und daß somit das gleiche für $R^{(i)}$ gilt, womit Satz I in allen Teilen bewiesen ist.

Eine Charakterisierung der Primideale vermöge des Dimensionsbegriffs wird gegeben durch

Satz II. *Ein Primideal besitzt keinen echten Teiler gleicher Höchstdimension; und umgekehrt wird jedes solche Ideal Primideal.*

Der Beweis beruht auf

Hilfssatz III. *Besitzt ein Primideal p aus Polynomen mit Koeffizienten aus einem Körper Ω nur endlichviele in bezug auf Ω linear unabhängige Restklassen, so hat p keinen vom Einheitsideal verschiedenen echten Teiler; m. a. W. das Restklassensystem nach p bildet einen Körper.*

Die Voraussetzung besagt, daß es eine endliche Zahl k gibt derart, daß zwischen je $(k + 1)$ Restklassen eine lineare Abhängigkeit mit Koeffizienten aus Ω besteht — genauer mit Koeffizienten aus dem durch alle Elemente von Ω repräsentierten Restklassenkörper (Ω) , daß aber mindestens ein System von k in bezug auf (Ω) linear unabhängigen Restklassen existiert; daraus folgt sofort, daß sich alle Restklassen linear durch ein beliebiges System von k linear unabhängigen ausdrücken lassen. — Sei jetzt a ein echter Teiler von p , $a(z) \not\equiv 0(p)$ ein Polynom aus a ; aus $c_1 f_1(z) + \dots + c_k f_k(z) \equiv 0(p)$ folgt dann auch $c_1 a(z) f_1(z) + \dots + c_k a(z) f_k(z) \equiv 0(p)$; das heißt aber, daß neben den Restklassen von $f_1, \dots, f_k$ auch die von $a f_1, \dots, a f_k$ ein System von k linear unabhängigen bilden, durch die sich also insbesondere die Einheitsklasse linear darstellen läßt. Es wird also a gleich dem Einheitsideal; anders ausgedrückt, das Restklassensystem bildet einen Körper, da es zu $a(z) \not\equiv 0(p)$ immer ein $f(z)$ gibt, so daß $1 \equiv a(z) f(z)(p)$ wird.

Zum Beweise des ersten Teiles von Satz II ist jetzt nur zu bemerken, daß jedes Primideal vor der Dimension $(n - i)$ — allgemeiner jedes Ideal von der Höchstdimension $(n - i)$ — nur endlich viele in bezug auf $P(u; x_{i+1}, \dots, x_n)$ linear unabhängige Restklassen besitzt, nämlich (§ 1, 5.) so viele wie der Grad von $R^{(i)}$ angibt, da g_{i-1} hier gleich dem Einheitsideal wird. Jeder echte Teiler a von p geht also bei Adjunktion von $x_{i+1}, \dots, x_n$ zu $P(u)$ in das Einheitsideal über; anders ausgedrückt, das Grundideal i -ter Stufe von a wird gleich dem Einheitsideal; das heißt

aber, daß die Höchstdimension von a höchstens gleich $n - i - 1$ wird. Damit die Aussage auch für ein nichttransformiertes Ideal a als Teiler gilt, hat man nur nach § 1, 2. zu einem neuen transformierten Bereich überzugehen.

Besitze jetzt umgekehrt p keinen echten Teiler gleicher Höchstdimension $n - i$; und sei $a \not\equiv 0(p)$, $b \not\equiv 0(p)$, wo a und b wieder als transformierte Ideale angenommen sind. Dann kommt nach Voraussetzung, da (a, p) und (b, p) als größte gemeinsame Teiler — im Idealsinn — echte Teiler von p werden:

$$G^{(i+1)} \equiv 0(a, p); \quad H^{(i+1)} \equiv 0(b, p); \quad G^{(i+1)} \not\equiv 0; \quad H^{(i+1)} \not\equiv 0.$$

Das ergibt aber

$$G^{(i+1)} H^{(i+1)} \equiv 0(ab, p); \quad G^{(i+1)} H^{(i+1)} \not\equiv 0;$$

und somit folgt notwendig $ab \equiv 0(p)$, da sonst p von geringerer Höchstdimension als $n - i$ wäre. Da a, b transformierte Ideale sind, ergibt sich also $\bar{p}$ und nach Hilfssatz I auch p als Primideal, womit Satz II bewiesen ist.

§ 3.

Nullstellen der Primideale und Primär ideale.

Den Übergang zu einer direkten Begründung der Theorie der Nullstellen (§ 1, 9.), vorerst für Primideale, bildet der eine Erweiterung von Hilfssatz III darstellende und für Primideale in beliebigen Ringen gültige

Hilfssatz IV. *Das Restklassensystem nach jedem vom Einheitsideal verschiedenen Primideal läßt sich durch Quotientenbildung zu einem Körper erweitern, dem Restklassenkörper des Primideals.*

Das Restklassensystem nach einem beliebigen Ideal bildet einen Ring, da Summe, Differenz und Produkt wieder dem System angehören, und assoziatives, kommutatives und distributives Gesetz beim Übergang zu den Restklassen erhalten bleiben. Handelt es sich speziell um Primideale, so besitzt dieser Ring keine Nullteiler; denn die Definition der Primideale (§ 1, 11.) sagt aus, daß das Produkt nicht verschwindender Restklassen ebenfalls nicht verschwindet. Ist das Primideal vom Einheitsideal verschieden, so enthält dieser Ring mindestens ein vom Nullelement verschiedenes Element, und läßt sich daher durch Quotientenbildung — Adjunktion von Elementenpaaren — zum Körper erweitern¹¹⁾; somit ist der Restklassenkörper definiert.

¹¹⁾ Steinitz, § 3. Die Annahme eines von Null verschiedenen Elementes im ursprünglichen Integritätsbereich genügt, da dann die Existenz der Einheit durch Quotientenbildung gesichert ist, und somit der ursprüngliche Bereich ein Teilbereich des Körpers wird; Steinitz setzt Existenz der Einheit im Integritätsbereich voraus.

Dem folgenden vorausgeschickt sei die durchweg festgehaltene

Bezeichnung: Restklassen sollen allgemein durch Klammersetzen irgendeines Elementes der Klasse bezeichnet werden, $(x)\dots, (a(x))\dots$; ebenso sollen Körper aus Restklassen durch Klammern bezeichnet werden. Insbesondere bezeichne $(P), (P(u)), (P(u, x_{i+1}, \dots, x_n))$ die Restklassenkörper, die aus allen und nur den Restklassen bestehen, die durch Elemente aus $P, P(u), P(u, x_{i+1}, \dots, x_n)$ repräsentiert werden können.

Weiter vorausgeschickt sei noch das folgende: Ein Körper $\mathfrak{K}$ heißt vom *algebraischen Rang* (Transzendenzgrad) k in bezug auf einen Grundkörper Ω , wenn $\mathfrak{K}$ mindestens ein System von k in bezug auf Ω algebraisch unabhängigen Größen — transzendenten Größen — enthält, wenn aber je $k+1$ Größen aus $\mathfrak{K}$ algebraisch abhängig in bezug auf Ω sind. Läßt sich $\mathfrak{K}$ als algebraischer Erweiterungskörper eines Teilkörpers $\Omega(z_1, \dots, z_s)$ darstellen, wo die z algebraisch unabhängig — transzendent — in bezug auf Ω sind, so wird notwendig s gleich k ; ¹²⁾ ebenso wird der algebraische Rang von $\mathfrak{K}(u)$ in bezug auf $\Omega(u)$ gleich k , wenn u nicht in $\mathfrak{K}$ enthaltene Unbestimmte bedeuten.

Die Konstruktion des Nullstellenkörpers geschieht jetzt in voller Analogie mit dem bei Primfunktionen einer Unbestimmten üblichen Weg ¹³⁾ nach

Satz III. *Dem Restklassenkörper $(\mathfrak{K})$ eines Primideals $\mathfrak{p}$ von der Dimension $n-i$ läßt sich isomorph ein Nullstellenkörper $\mathfrak{K}$ von $\mathfrak{p}$ zuordnen, der vom algebraischen Rang $n-i$ wird — von $n-i$ Parametern abhängt — und insbesondere als endlicher Erweiterungskörper von $P(u, x_{i+1}, \dots, x_n)$ aufgefaßt werden kann. Der Isomorphismus zwischen $(\mathfrak{K})$ und $\mathfrak{K}$ umfaßt denjenigen zwischen (P) und $P, (P(u))$ und $P(u)$ und bei Zugrundelegung der $x_{i+1}, \dots, x_n$ als Parameter auch den zwischen $(P(u, x_{i+1}, \dots, x_n))$ und $P(u, x_{i+1}, \dots, x_n)$. Umgekehrt ist jeder Nullstellenkörper vom algebraischen Rang $n-i$ — von $n-i$ Parametern abhängig — dem Restklassenkörper $(\mathfrak{K})$ isomorph.*

Satz III ergibt als Korollar den bekannten Satz: Verschwindet ein Ideal α in allen Nullstellen eines Primideals $\mathfrak{p}$, so wird α durch $\mathfrak{p}$ teilbar.

Zum Beweise ist vorerst zu bemerken, daß der Restklassenkörper $(\mathfrak{K})$ vom algebraischen Rang $n-i$ in bezug auf $(P(u))$ wird. Denn die

¹²⁾ Für einen bei beliebiger Charakteristik gültigen Beweis dieser bekannten Tatsache vgl. Steinitz, § 22, 9. — Bei Adjunktion der u kann der algebraische Rang nicht zunehmen, da es sich um rationale Verbindungen der ursprünglichen Elemente mit Koeffizienten aus $\Omega(u)$ handelt; nicht abnehmen, da jede Relation zwischen Elementen aus $\mathfrak{K}$ mit Koeffizienten aus $\Omega(u)$ in endlich viele Relationen mit Koeffizienten aus Ω zerfällt.

¹³⁾ Steinitz, § 6.

Klassen $(x_{i+1}), \dots, (x_n)$ sind in bezug auf $(P(u))$ algebraisch unabhängig, da $\mathfrak{p}$ als von der Dimension $n-i$ kein von $x_1, \dots, x_i$ freies Polynom enthält; jede weitere Klasse aber ist von diesen abhängig. Denn aus der Zugehörigkeit der Elementarteilerform $P^{(i)}$ zu $\mathfrak{p}$ folgt nach § 1, 2. auch für $\lambda = 1, 2, \dots, i$ die Zugehörigkeit von Polynomen, die jeweils von $x_\lambda, x_{i+1}, \dots, x_n$ abhängig sind. $(\mathfrak{K})$ wird also ein endlicher Erweiterungskörper von $(P(u, x_{i+1}, \dots, x_n))$; der Grad in bezug auf diesen Teilkörper wird nach § 1, 5. — unter Berücksichtigung, daß $\mathfrak{g}_{i-1}$ gleich dem Einheitsideal, $\mathfrak{g}_i$ nach Satz I gleich $\mathfrak{p}$ wird — gleich dem Grad der Norm.

Um zu einem isomorphen Nullstellenkörper überzugehen, ist weiter zu bemerken, daß $P(u, x_{i+1}, \dots, x_n)$ und $(P(u, x_{i+1}, \dots, x_n))$ isomorph aufeinander bezogen sind dadurch, daß jedem Element aus $P(u, x_{i+1}, \dots, x_n)$ die durch das Element repräsentierte Restklasse zugeordnet wird. Denn vorerst entsprechen sich bei dieser Zuordnung die aus den Polynomen in $x_{i+1}, \dots, x_n$ bzw. in $(x_{i+1}), \dots, (x_n)$ bestehenden Integritätsbereiche isomorph, da in $\mathfrak{p}$ kein von $x_1, \dots, x_i$ freies Polynom enthalten ist, verschiedenen Polynomen aus $P(u, x_{i+1}, \dots, x_n)$ also auch verschiedene Klassen entsprechen; aus isomorphen Integritätsbereichen gehen aber durch Quotientenbildung isomorphe Körper hervor. Die isomorphe Beziehung zwischen $P(u, x_{i+1}, \dots, x_n)$ und $(P(u, x_{i+1}, \dots, x_n))$ umfaßt diejenige zwischen P und (P) , $P(u)$ und $(P(u))$. Um diesen Isomorphismus zu einem solchen zwischen $(\mathfrak{K})$ und einem Nullstellenkörper $\mathfrak{K}$ zu erweitern, seien den Klassen $(x_1), \dots, (x_i)$ gewisse neue Elemente $\bar{x}_1, \dots, \bar{x}_i$ isomorph zugeordnet; d. h. jedem Polynom $(a(x))$ entspreche ein Polynom $a(\bar{x}_1, \dots, \bar{x}_i, x_{i+1}, \dots, x_n)$; Summe und Produkt entspreche Summe und Produkt. Durch Quotientenbildung — wobei man sich auf Nenner aus dem Teilkörper $(P(u, x_{i+1}, \dots, x_n))$ bzw. $P(u, x_{i+1}, \dots, x_n)$ beschränken kann — entspricht dann dem Restklassenkörper $(\mathfrak{K})$ ein Körper $\mathfrak{K}$, der endliche Erweiterung von $P(u, x_{i+1}, \dots, x_n)$ vom Grade der Norm wird, und der als Nullstellenkörper bezeichnet werden kann; denn die Zuordnung sagt aus, daß $f(\bar{x}_1, \dots, \bar{x}_i, x_{i+1}, \dots, x_n)$ verschwindet, sobald $f(x) \equiv 0 (\mathfrak{p})$ wird. An Stelle von $(P(u, x_{i+1}, \dots, x_n))$ könnte bei der ganzen Überlegung auch irgendein anderer, durch Adjunktion von $n-i$ algebraisch unabhängigen Größen entstehender Teilkörper von $(\mathfrak{K})$ treten.

Umgekehrt ist leicht zu zeigen, daß jeder Nullstellenkörper $\mathfrak{K}$ vom algebraischen Rang $n-i$ dem Restklassenkörper isomorph wird. Da sich $\mathfrak{K}$ rational, mit Koeffizienten aus $P(u)$, aus den Größen $\bar{x}_1, \dots, \bar{x}_n$ ableiten läßt, müssen unter diesen Größen $n-i$ algebraisch unabhängige, also in bezug auf $P(u)$ transzendente Elemente enthalten sein. Insbesondere muß dies für $\bar{x}_{i+1}, \dots, \bar{x}_n$ erfüllt sein, da wegen $P^{(i)} \equiv 0 (\mathfrak{p})$ wie oben folgt, daß $\mathfrak{K}$ ein algebraischer Erweiterungskörper von $P(u, \bar{x}_{i+1}, \dots, \bar{x}_n)$

wird. Da nach Voraussetzung $f(\bar{x})$ verschwindet für jedes Polynom $f(x)$ aus $\mathfrak{p}$, entspricht jeder Klasse des in $(\mathfrak{K})$ enthaltenen Polynombereichs der (x) ein und nur ein Element aus $\mathfrak{K}$, das ein Polynom in den $\bar{x}$ wird; und Summe und Produkt entsprechen Summe und Produkt. Es entsprechen aber verschiedenen Klassen auch verschiedene Elemente aus $\mathfrak{K}$; denn sonst würde einer von Null verschiedenen Klasse, also nach geeigneter Multiplikation auch einer durch ein Polynom repräsentierten Klasse aus $(P(u, x_{i+1}, \dots, x_n))$ das Element Null in $\mathfrak{K}$ entsprechen, zwischen den Größen $\bar{x}_{i+1}, \dots, \bar{x}_n$ bestünde entgegen der Voraussetzung eine algebraische Abhängigkeit. Durch diese Zuordnung werden alle in $\mathfrak{K}$ enthaltene Polynome der $\bar{x}$ erschöpft; durch Quotientenbildung — wobei man sich wieder auf Nenner aus $(P(u, x_{i+1}, \dots, x_n))$, bzw. $P(u, \bar{x}_{i+1}, \dots, \bar{x}_n)$ beschränken kann — gehen aber aus diesen isomorphen Integritätsbereichen isomorphe Körper hervor.

Das Ideal $\mathfrak{a}$ verschwinde jetzt in allen Nullstellen von $\mathfrak{p}$, also insbesondere auch in allen von $n - i$ Parametern abhängigen. Ist dann $a(x)$ ein beliebiges Polynom aus $\mathfrak{a}$, so verschwindet also $a(\bar{x})$; wegen des Isomorphismus zwischen $\mathfrak{K}$ und $(\mathfrak{K})$ wird somit $(a(x))$ die Nullklasse, $\mathfrak{a}(x)$ und somit $\mathfrak{a}$ durch $\mathfrak{p}$ teilbar. Damit ist Satz III und Korollar bewiesen.

Um von Satz III zu der in § 1, 9. gegebenen Zerlegung zunächst für Primideale überzugehen, und um genauere Aussagen über die Exponenten machen zu können, bedarf es einer weiteren Untersuchung der Elementarteilerform nach

Hilfssatz V. Ist bei Charakteristik p die Elementarteilerform $E^{(i)}$ eines Primideals oder Primärideals — allgemeiner eines Ideals $\mathfrak{a}$, bei dem die Höchstdimension mit der Dimension schlechthin zusammenfällt — vom Exponenten f in bezug auf x_i , also ganze Funktion von $x_i^{p^f}$, so ist sie auch vom Exponenten f in bezug auf $x_{i+1}, \dots, x_n$ und auf die in $E^{(i)}$ auftretenden Unbestimmten u_μ , bzw. t_μ . Insbesondere ist also bei vollkommenem Körper als Koeffizientenbereich die Elementarteilerform $P^{(i)}$ eines Primideals stets vom Exponenten Null in bezug auf x_i , also eine Primfunktion erster Art.

Dazu ist zu bemerken, daß $P(u, x_{i+1}, \dots, x_n)$ unvollkommen wird, sobald P ein vollkommener Körper von der Charakteristik p ist, so daß aus § 1, 14. nicht direkt folgt, daß $P^{(i)}$ erster Art wird. Sei jetzt $E^{(i)}$ vom Exponenten f in bezug auf x_i , enthalte aber eine andere Unbestimmte x_{i+1} zum Exponenten $f' < f$. Dann gibt es — durch Vertauschen der u_μ , bzw. t_μ — nach § 1, 2. auch ein von Null verschiedenes durch das Ideal teilbares Polynom $G^{(i)}$, das ganze Funktion von $x_i^{p^{f'}}$ wird, und das nach Definition der Elementarteilerform durch $E^{(i)}$ teilbar wird. Da aber $G^{(i)}$

von gleichem Grad wie $E^{(i)}$ wird, muß es bis auf eine Größe aus $P(u)$ als Faktor mit $E^{(i)}$ übereinstimmen, und somit wird notwendig f' gleich f . Damit wird aber $E^{(i)}$ — das als ganz und primitiv in den t_{μ} vorausgesetzt werden darf — von der Form

$$E^{(i)} = \sum c_i(t) x_i^{p^f} \dots x_n^{p^f} = \sum c_i(t) g_i(y^{p^f}, t^{p^f}) = \sum T_\mu(t) \bar{h}_\mu(y^{p^f}),$$

wo die T_μ Potenzprodukte der t bedeuten, und die $\bar{h}$ durch $\bar{a}$ teilbar werden. Daher erhält man ein ebenfalls zu $\bar{a}$ gehörendes Polynom, wenn in den T_μ jeder Exponent der einzelnen t durch das größte darin enthaltene Vielfache von p^f ersetzt wird; das kommt aber, wie die obige Darstellung ablesen läßt, darauf hinaus, in $c_i(t)$ jeden Exponenten der t durch das größte darin enthaltene Vielfache von p^f zu ersetzen. Durch diese Substitution geht $E^{(i)}$ über in ein Polynom der $t, x_i, \dots, x_n$, das nach Definition durch $E^{(i)}$ teilbar wird, und zwar wegen der vorausgesetzten Primitivität auch in bezug auf die t ; es muß also mit $E^{(i)}$ identisch werden, da der Grad in keinem Argumente zugenommen hat. Ist insbesondere P ein vollkommener Körper, so wird also $E^{(i)}$ als ganze Funktion von x^{p^f}, t^{p^f} eine p^f -te Potenz; handelt es sich daher um ein Primideal, so muß notwendig f gleich Null werden; die Elementarteilerform $P^{(i)}$ wird eine Primfunktion erster Art.

Die Zerlegung wird jetzt gegeben durch

Satz IV. Die Elementarteilerform $P^{(i)}$ eines Primideals läßt in dem aus dem Nullstellenkörper abgeleiteten Galoisschen Körper die explizite Zerlegung zu:

$$\begin{aligned} P^{(i)} &= \prod (x_i - t_{1i} \bar{y}_{1v} - \dots - t_{ni} \bar{y}_{nv})^\delta \\ &= \prod (t_{1i}(y_1 - \bar{y}_{1v}) + \dots + t_{ni}(y_n - \bar{y}_{nv}))^\delta, \end{aligned}$$

wo $\bar{y}_{1v}, \dots, \bar{y}_{nv}$ je ein zusammengehöriges von $t_{1i}, \dots, t_{ni}$ unabhängiges Nullstellensystem der ursprünglichen Unbestimmten y darstellt, verschiedenen v verschiedene Linearfaktoren entsprechen und wo der Exponent δ bei vollkommenem Körper P den Wert Eins, bei unvollkommenem den Wert p^f ($f \geq 0$) hat. Dadurch ist bei Adjunktion neuer Unbestimmten v die Zerlegung der in bilinearen Verbindungen der u und v an Stelle der u_{μ} geschriebenen Elementarteilerform mitbestimmt:

$$P^{(i)}(u, v) = \prod (z - v_1 \bar{x}_{1v} - \dots - v_i \bar{x}_{iv})^\delta,$$

wo δ die gleiche Bedeutung wie oben hat. Ebenso ist die Zerlegung der Norm eines Primideals oder eines Primärideals mit $\mathfrak{p}$ als zugehörigem Primideal — als Potenz von $P^{(i)}$ — mitgegeben.

Als Korollar aus Satz IV kommt noch: Stimmen zwei Primideale in ihrer Elementarteilerform $P^{(i)}$ überein, so sind sie identisch.

Der Beweis von Satz IV wird auf den Nachweis hinauskommen, daß die Elementarteilerform $P^{(i)}$ mit der Fundamentalgleichung des Erweiterungskörpers $(P(u, x_i, x_{i+1}, \dots, x_n))$ von $(P(u, x_{i+1}, \dots, x_n))$ identisch ist. Vor-erst gehe man — um Einblick in die Abhängigkeit von den Unbestimmten $u_{\mu\nu}$ bzw. $t_{\mu\nu}$ zu gewinnen — auf den Restklassenkörper $(\bar{\mathfrak{R}})$ von $\bar{\mathfrak{p}}$ über, der nach dem bei der Definition des algebraischen Rangs Gesagten vom algebraischen Rang $n - i$ in bezug auf $(\bar{P})$ werden muß, wo $(\bar{P})$ den durch Elemente aus P repräsentierten Teilkörper bedeutet. Denn $(\bar{\mathfrak{R}})$ entsteht durch Adjunktion der Unbestimmten u bzw. t zu einem $(\bar{\mathfrak{R}})$ isomorphen Teilkörper, der durch Quotientenbildung aus allen und nur den Klassen hervorgeht, die durch Polynome aus $\bar{\mathfrak{S}}$ repräsentiert werden können, wobei $(\bar{P})$ und (P) einander entsprechen. Der algebraische Rang von $(\bar{\mathfrak{R}})$ in bezug auf $(P(u))$ ist also gleich dem dieses Teilkörpers in bezug auf (P) , und somit wegen des Isomorphismus gleich dem von $(\bar{\mathfrak{R}})$ in bezug auf $(\bar{P})$. Da $(\bar{\mathfrak{R}})$ sich rational, mit Koeffizienten aus $(\bar{P})$, aus den Klassen $(y_1), \dots, (y_n)$ ableiten läßt, müssen also unter diesen Klassen $(n - i)$ algebraisch unabhängige sein, und $(\bar{\mathfrak{R}})$ entsteht als endlicher algebraischer Erweiterungskörper dieses durch Adjunktion der $(n - i)$ Klassen zu $(\bar{P})$ erzeugten Teilkörpers¹⁴⁾.

Adjungiert man nur die in $x_{i+1}, \dots, x_n$ auftretenden Unbestimmten $t_{\sigma\tau}$, so entsteht wieder ein Restklassenkörper, der die Klassen $(y_1), \dots, (y_n)$ und $(x_{i+1}), \dots, (x_n)$ enthält und endlicher algebraischer Erweiterungskörper von $(P(t_{\sigma\tau}, x_{i+1}, \dots, x_n))$ wird — es handelt sich dabei um Körper, die zu Teilkörpern von $(\bar{\mathfrak{R}})$ isomorph sind, nicht damit identisch; da bei verschiedenen Unbestimmten die Restklassen zwar durch dieselben Elemente repräsentiert werden, aber nicht identisch sind, da sie nicht die gleichen Elemente enthalten. Bei der Abhängigkeit der Klassen (y) von $(P(t_{\sigma\tau}, x_{i+1}, \dots, x_n))$ gehen also nur die Unbestimmten $t_{\sigma\tau}$ ein; man bilde jetzt, durch Adjunktion von $t_{1i}, \dots, t_{ni}$, die Klasse $(x_i) = (t_{1i}y_1 + \dots + t_{ni}y_n)$, und es seien $(x_{i\nu}) = (t_{1i}y_{1\nu} + \dots + t_{ni}y_{n\nu})$ die r verschiedenen konjugierten Werte, welche in dem in bezug auf $(P(t_{\sigma\tau}, t_{1i}, \dots, t_{ni}, x_{i+1}, \dots, x_n))$ Galoisschen Körper gelegen sind. Dann wird — je nachdem es sich um Erweiterungen erster Art handelt oder nicht — das Produkt über die Faktoren $t - (x_{i\nu})$ oder über ihre p^f -ten Potenzen eine Primfunktion (G) in bezug auf $(P(t, x_{i+1}, \dots, x_n))$; denn da es Elemente vom Grade $r \cdot p^f$

¹⁴⁾ Diese Bemerkung zeigt, daß Satz III mit Korollar direkt für den Nullstellenkörper $\bar{\mathfrak{R}}$ von $\bar{\mathfrak{p}}$ hätte ausgesprochen und bewiesen werden können. Durch den Übergang zum transformierten Ideal wird aber erst erreicht, daß in den größten primären Komponenten gleicher Dimension eines beliebigen Ideals bei den Nullstellen die gleichen Parameter auftreten; und damit ergibt sich erst der Zusammenhang mit Norm und Elementarteilerform eines beliebigen Ideals.

gibt (§ 1, 15.), muß notwendig (x_i) ein solches sein, da jedes Element durch Spezialisierung der $t_{1i}, \dots, t_{ni}$ entsteht; (x_i) wird aber Nullstelle von (G) . Geht man zu dem isomorphen Nullstellenkörper von $\mathfrak{p}$ und dem daraus abgeleiteten Galoisschen Körper über, so läßt also hier G eine Zerlegung in Linearfaktoren $t - t_{1i}\bar{y}_{1v} - \dots - t_{ni}\bar{y}_{nv}$ bzw. ihre p^f -ten Potenzen zu. Nun wird aber, da (G) für $t = (x_i)$ verschwindet, $G(x_i)$ durch $\mathfrak{p}$ und somit durch $P^{(i)}$ teilbar, und als Primfunktion in bezug auf $P(u, x_{i+1}, \dots, x_n)$ und als primitiv in $x_{i+1}, \dots, x_n$ mit $P^{(i)}$ identisch; somit ist die erste Zerlegung von Satz IV bewiesen.

Um zu der zweiten Zerlegung überzugehen, ist zu bemerken, daß die Eigenschaft, Erweiterung erster Art zu sein oder nicht, bei Adjunktion von Unbestimmten erhalten bleibt. Bildet man also, nach Adjunktion von $v_1, \dots, v_i$ und aller $t_{\mu v}$, die Klasse $(z) = (v_1 x_1 + \dots + v_i x_i)$ und die konjugierten Klassen $(z_v) = (v_1 x_{1v} + \dots + v_i x_{iv})$, so wird das Produkt über alle $t - (z_v)$ bzw. ihre p^f -ten Potenzen wieder eine Primfunktion (H) , die für $t = (z)$ verschwindet. Somit wird H wie oben als Produkt von Linearfaktoren darstellbar und mit der Elementarteilerform des aus $\mathfrak{p}$ durch Zusammensetzen der Transformation (1) mit $z = v_1 x_1 + \dots + v_i x_i$ abgeleiteten Primideals identisch; diese Elementarteilerform entsteht aber — wegen der gegenseitigen Spezialisierung — aus $P^{(i)}$ dadurch, daß die $u_{\mu v}$ durch gewisse bilineare Verbindungen der u und v ersetzt werden¹⁵⁾. Mit diesen Zerlegungen ist aber auch die Zerlegung der Norm als Potenz von $P^{(i)}$ mitgegeben¹⁶⁾, ebenso die von Norm und Elementarteilerform eines Primärals mit $\mathfrak{p}$ als zugehörigem Primideal.

Stimmen schließlich zwei Primideale in der Elementarteilerform $P^{(i)}$ überein, so stimmen sie als Folge der obigen Zerlegung in ihren Nullstellen überein, sind also gegenseitig durch einander teilbar und somit identisch.

§ 4.

Arithmetische Fassung des Dimensionsbegriffes.

Eine erste von der Einführung transformierter Ideale unabhängige Fassung des Dimensionsbegriffes ist gegeben durch

Satz V. *Die Dimension eines Primideals ist gegeben durch den algebraischen Rang seines Restklassenkörpers. Die Höchstdimension eines*

¹⁵⁾ Vgl. H.-N., § 7.

¹⁶⁾ Es handelt sich bei Erweiterungen erster Art, also insbesondere bei vollkommenen Körpern, um die erste Potenz; bei unvollkommenen Körpern aber um die p^0 -te Potenz, wie in § 6, Satz XIII und XIV, gezeigt werden wird.

Ideals ist gleich der höchsten der Dimensionszahlen seiner zugehörigen Primideale. ^A

Der erste Teil von Satz V war bewiesen in der ersten Bemerkung zu Satz IV, wo gezeigt war, daß der algebraische Rang des Restklassenkörpers $(\bar{\mathfrak{R}})$ von $\bar{\mathfrak{p}}$ gleich dem des Restklassenkörpers $(\mathfrak{R})$ von $\mathfrak{p}$ wird, also gleich der Dimension von $\mathfrak{p}$ in Übereinstimmung mit § 1, 8. Zum Beweis des zweiten Teiles sei $m = [q_1, \dots, q_a]$ eine kürzeste Darstellung durch größte primäre Komponenten; dann kann vorerst kein q , als Teiler von m , höhere Dimension besitzen als m . Das Produkt aller q wird aber durch m teilbar, und somit auch das Produkt aller Elementarteilerformen der einzelnen q ; ist somit $(n-i)$ die höchste der Dimensionszahlen der q , so enthält m ein Polynom $G^{(i)} \neq 0$, kann also auch nicht von höherer Dimension sein als $n-i$. Die Dimensionszahlen der q stimmen aber nach Satz I mit denen ihrer zugehörigen Primideale überein. Definiert man ohne Einführung transformierter Ideale die Dimension eines Primideals durch den algebraischen Rang des Restklassenkörpers, so gibt der zweite Teil von Satz V die Definition der Höchstdimension eines beliebigen Ideals.

Um den Dimensionsbegriff andererseits durch Ketten von Primidealen fassen zu können, was wieder unabhängig von der Einführung transformierter Ideale wird, ist in Ergänzung von Satz II zu zeigen:

Satz VI. Jedes vom Einheitsideal verschiedene Primideal besitzt — nach eventueller Adjunktion von Unbestimmten — mindestens ein Primideal als Teiler, dessen Dimension um genau eine Einheit abgenommen hat.

Ist nämlich $\mathfrak{p}$ von der Dimension $(n-i) > 0$ und bedeutet v eine neue Unbestimmte, so wird $c = (\mathfrak{p}, x_i - v)$ ein Ideal von der gesuchten Eigenschaft. Das folgt aus einer isomorphen Zuordnung; es kommt $c = (\mathfrak{p}^*, x_i - v)$, wo $\mathfrak{p}^*$ aus $\mathfrak{p}$ dadurch entstanden ist, daß x_i durch die Unbestimmte v ersetzt ist und v dem Koeffizientenbereich adjungiert wird; ebenso entstehen die Restklassen durch Ersetzen der Klasse (x_i) durch (v) . Nun geht aber $\mathfrak{p}$ in sich über, wenn x_i zu $P(u)$ adjungiert wird; aus $h(x_i)f(x) \equiv 0(\mathfrak{p})$, $h(x_i) \neq 0$ folgt nämlich notwendig $f(x) \equiv 0(\mathfrak{p})$; denn enthielte $\mathfrak{p}$ ein nur von x_i abhängiges Polynom, so enthielte es auch ein nur von x_n abhängiges, wäre also gegen Voraussetzung höchstens von der Dimension Null. Bei der Zuordnung $v \sim x_i$ entspricht also der Nullklasse nach c notwendig die Nullklasse nach $\mathfrak{p}$, und natürlich gilt auch das Umgekehrte. Somit ergibt sich eine isomorphe Zuordnung zwischen dem Restklassensystem nach $\mathfrak{p}$ und c ; letzteres besitzt also keine Nullteiler, c wird Primideal. Vermöge dieser isomorphen Zuordnung entspricht der algebraischen Abhängigkeit zwischen (x_i) und $(P(u, x_{i+1}, \dots, x_n))$ eine Relation

zwischen $(x_{i+1}), \dots, (x_n)$ in bezug auf $(P(u, v))$, während für $\lambda = 1, \dots, i-1$ die Abhängigkeiten zwischen (x_λ) und $(P(u, x_{i+1}, \dots, x_n))$ als solche erhalten bleiben und daher den algebraischen Rang nicht weiter erniedrigen; der algebraische Rang hat um genau eine Einheit abgenommen. War $\mathfrak{p}$ von der Dimension Null, so wird $\mathfrak{c}$ das Einheitsideal; das obige Resultat bleibt also erhalten. Im ursprünglichen Bereich $\mathfrak{S}$ wird somit $\bar{\mathfrak{a}} = (\bar{\mathfrak{p}}, v + v_1 y_1 + \dots + v_n y_n)$, wo v_i für $-t_i$ gesetzt ist, ein Ideal von der gesuchten Beschaffenheit. Enthält P insbesondere unendlich viele Elemente, so lassen sich $v, v_1, \dots, v_n$ immer so zu Elementen aus P spezialisieren, daß Norm und Elementarteilerform und somit die Dimension von $\mathfrak{a}$ gleich wird der des spezialisierten Ideals $\mathfrak{b}^{17)}$, wobei die Elementarteilerform allerdings nicht Primfunktion zu bleiben braucht. Nach Satz V besitzt aber $\mathfrak{b}$ mindestens ein zugehöriges Primideal der gesuchten Dimension; geht man wieder zu $\mathfrak{S}$ zurück, so gilt hier also Satz VI ohne Adjunktion irgendwelcher Unbestimmten.

Satz II und Satz VI ergeben unmittelbar die gewünschte Fassung nach

Satz VII. *Ein Primideal $\mathfrak{p}$ ist von der Dimension $n-i$, wenn es — bei eventueller Adjunktion von Unbestimmten — mindestens eine Kette von $1 + (n-i) + 1$ Primidealen gibt*

$$\mathfrak{p}_0 = \mathfrak{p}; \mathfrak{p}_1, \dots, \mathfrak{p}_{n-i}; \mathfrak{p}_{n-i+1} \subsetneq \mathfrak{p}_{n-i+2} \subsetneq \dots$$

von denen jedes ein echter Teiler des unmittelbar vorangehenden ist, wenn aber keine derartige Kette von größerer Gliederzahl existiert. Diese Definition gilt auch im ursprünglichen Bereich, und zwar ohne Einführung irgendwelcher Unbestimmten, wenn P unendlich viele Elemente enthält¹⁸⁾.

Vorerst ist klar, daß das letzte Element der Kette gleich dem Einheitsideal werden muß — das der Definition des Primideals genügt —, da sich sonst die Kette durch Zufügung von $\mathfrak{o}$ verlängern ließe; für $\mathfrak{o}$ selbst ergibt sich nach Satz VII die Dimension -1 in Übereinstimmung mit § 1, 8. Sei jetzt $\mathfrak{p}$ von $\mathfrak{o}$ verschieden und von der Dimension $n-i$, so kann die Gliederzahl der Kette höchstens $1 + (n-i) + 1$ betragen, da nach Satz II nicht zwei Primideale gleicher Dimension auftreten können. Es existiert aber nach Satz VI — bei eventueller Adjunktion neuer Unbestimmten — mindestens eine Kette dieser Gliederzahl, indem die Di-

¹⁷⁾ Vgl. H.-N., letzter Absatz von § 7.

¹⁸⁾ Diese Kettendefinition der Dimension ergibt im Fall des algebraischen Zahlkörpers die Dimension Null für die gewöhnlichen Primideale, die Dimension -1 für das Einheitsideal und die Dimension 1 für das Nullideal; tatsächlich genügt ja auch letzteres der Definition der Primideale — im Körper ist ein Produkt von nicht verschwindenden Größen stets von Null verschieden. Satz II bleibt bei dieser Definition der Dimension im algebraischen Zahlkörper erhalten.

mension bei jedem Glied der Kette um genau eine Einheit abgenommen hat. Legt man Satz VII als Definition der Dimension zugrunde — eine Definition, die sich offenbar genau gerade so im ursprünglichen Bereich aussprechen läßt und bei der nach Satz VI die Einführung von Unbestimmten unnötig wird, wenn P unendlich viele Elemente besitzt —, so ist die Definition der Höchstdimension eines beliebigen Ideals wieder durch den zweiten Teil von Satz V gegeben. 

§ 5.

Einordnung der Grundideale und ihrer Komponenten in die allgemeine Idealtheorie. Nullstellen der Ideale.

Es handelt sich um die Charakterisierung der Grundideale und ihrer Komponenten (§ 1, 7.) durch isolierte Komponenten der Zerlegung (§ 1, 13.) im Sinne der allgemeinen Idealtheorie. Diese Charakterisierung wird das Parallelgehen der Zerlegungssätze der Normen mit denen der allgemeinen Idealtheorie zeigen und wird gestatten, die in § 3 für Primideale und Primärideale gegebene Theorie der Nullstellen für beliebige Ideale auszusprechen. Für die Grundideale gilt

Satz VIII. *Die Grundideale i -ter Stufe g_i sind die isolierten Komponenten der Zerlegung, die eindeutig bestimmt sind durch die Gesamtheit der zugehörigen Primideale der Dimensionen $n-1, n-2, \dots, n-i$. Sind alle zugehörigen Primideale von derselben Dimension, so wird auch das Ideal von dieser Dimension; d. h. es tritt nur ein Faktor $R^{(i)}$ der Norm auf; allgemein besitzt die Norm so viele von der Einheit verschiedene Faktoren $R^{(i)}, R^{(i+\sigma)}, R^{(i+\tau)}, \dots$, als verschiedene Dimensionszahlen unter den zugehörigen Primidealen auftreten.*

Dem Beweise vorausgeschickt sei

Hilfssatz VI. *Ist ein Ideal dargestellt als kleinstes gemeinsames Vielfaches, $m = [a_1, \dots, a_a]$, so wird sein Grundideal g_i kleinstes gemeinsames Vielfaches der Grundideale i -ter Stufe h_i der a .*

Denn aus

$$b^{(i+1)} f \equiv 0(m), \quad b^{(i+1)} \neq 0 \quad \text{folgt} \quad b^{(i+1)} f \equiv 0(a_i), \quad b^{(i+1)} \neq 0;$$

es wird also g_i durch $[h_{i1}, \dots, h_{ia}]$ teilbar. Umgekehrt folgt aus

$$c_i^{(i+1)} f \equiv 0(a_i), \quad c_i^{(i+1)} \neq 0$$

auch

$$c_1^{(i+1)} \dots c_a^{(i+1)} f \equiv 0(m), \quad c_1^{(i+1)} \dots c_a^{(i+1)} \neq 0,$$

und damit die umgekehrte Teilbarkeit, womit der Hilfssatz bewiesen ist.

Seien jetzt die zugehörigen Primideale von $\mathfrak{m}$ nach der Dimension angeordnet (wo natürlich gewisse Dimensionen auch fehlen können, $j_\lambda = 0$)

$$\mathfrak{p}_{1,1}, \dots, \mathfrak{p}_{1,j_1}; \mathfrak{p}_{2,1}, \dots, \mathfrak{p}_{2,j_2}; \dots; \mathfrak{p}_{n,1}, \dots, \mathfrak{p}_{n,j_n},$$

wo allgemein $\mathfrak{p}_{\lambda,\kappa}$ ein Primideal der Dimension $n - \lambda$ bezeichnet; $\mathfrak{q}_{\lambda,\kappa}$ sei das in einer festen gegebenen Zerlegung von $\mathfrak{m}$ auftretende entsprechende primäre Ideal. Dann wird das Grundideal i -ter Stufe nach Definition gleich dem Einheitsideal für alle $\mathfrak{q}_{\lambda,\kappa}$, für die $\lambda > i$ ist; für $\lambda \leq i$ aber wird nach Satz I dieses Grundideal gleich $\mathfrak{q}_{\lambda,\kappa}$. Somit kommt nach Hilfssatz VI:

$$(5) \quad \mathfrak{g}_i = [\mathfrak{q}_{1,1}, \dots, \mathfrak{q}_{1,j_1}; \dots; \mathfrak{q}_{i,1}, \dots, \mathfrak{q}_{i,j_i}],$$

und diese Darstellung läßt $\mathfrak{g}_i$ als isolierte Komponente der Zerlegung erkennen, da keines der zu $\mathfrak{g}_i$ gehörigen Primideale in einem der übrigen Primideale, die sämtlich von niedrigerer Dimension sind, aufgehen kann.

Treten speziell unter den zugehörigen Primidealen nur solche der Dimension $n - i$ auf, so wird $\mathfrak{g}_0, \dots, \mathfrak{g}_{i-1}$ nach (5) gleich dem Einheitsideal, $\mathfrak{g}_i = \mathfrak{g}_{i+1} = \dots = \mathfrak{m}$; es wird also $R_{\mathfrak{m}} = R^{(i)}$. Sind aber Primideale verschiedener Dimension vorhanden, ist etwa $j_i, j_{i+\sigma}, j_{i+\tau}, \dots$ von Null verschieden, so wird nach (5):

$$\mathfrak{g}_0 \neq \mathfrak{g}_i \neq \mathfrak{g}_{i+\sigma} \neq \mathfrak{g}_{i+\tau} \neq \dots,$$

aber

$$\mathfrak{g}_0 = \mathfrak{g}_1 = \dots = \mathfrak{g}_{i-1} = \mathfrak{o}, \quad \mathfrak{g}_i = \mathfrak{g}_{i+1} = \dots = \mathfrak{g}_{i+\sigma-1}, \dots$$

es werden also die Faktoren $R^{(i)}$, $R^{(i+\sigma)}$, $R^{(i+\tau)}$ und nur diese von der Einheit verschieden¹⁹⁾.

Vermöge Satz VIII läßt sich Satz I verschärfen zu

Satz IX. *Ein Ideal ist dann und nur dann primär, wenn seine Elementarteilerform — und folglich seine Norm — eine Primärfunktion ist.*

Daß die Bedingung für primäre Ideale erfüllt ist, war in Satz I gezeigt. Sei jetzt umgekehrt die Elementarteilerform von $\mathfrak{m}$ gegeben durch $Q^{(i)} = (P^{(i)})^e$, wo $P^{(i)}$ eine Primfunktion bedeutet. Dann sind nach Satz VIII alle Primideale von $\mathfrak{m}$ von derselben Dimension $n - i$. Aus $\mathfrak{m} = [\mathfrak{q}_1, \dots, \mathfrak{q}_a]$ ergibt sich:

$$Q^{(i)} \equiv 0(\mathfrak{q}_\lambda); \text{ also } (P^{(i)})^e \equiv 0(\mathfrak{p}_\lambda) \text{ und somit } P^{(i)} \equiv 0(\mathfrak{p}_\lambda).$$

¹⁹⁾ Aus Satz VIII ergibt sich wieder unter Beachtung von Hilfssatz II, daß die Grundideale — als kleinste gemeinsame Vielfache von transformierten Idealen — transformierte Ideale werden. Da Satz VIII nur auf Sätzen aus H.-N. beruht, wo diese Tatsache nicht benutzt wird, so ergibt sich damit ein neuer Beweis, der zugleich den inneren Grund aufdeckt. Der Satz wird bei H.-N. nur bei der Theorie der Nullstellen verwendet, die ja hier neu entwickelt ist.

Da nun alle p_λ von der Dimension $n - i$ sind, und $P^{(i)}$ eine Primfunktion bedeutet, so wird $P^{(i)}$ gleich der Elementarteilerform von jedem p_λ . Somit stimmen nach dem Korollar zu Satz IV alle p_λ überein; es kann also, da es sich um größte primäre Komponenten handelt, nur ein p auftreten; m wird primär, wobei für $\varrho = 1$ der Spezialfall prim nicht ausgeschlossen ist. Satz VIII und Satz IX führen zur Einordnung der Komponenten der Grundideale nach

Satz X. Die Komponente r_λ des Grundideals g_i , die dem größten primären Faktor $Q_\lambda^{(i)} = (P_\lambda^{(i)})^{e_\lambda}$ von $R^{(i)}$ entspricht, ist gegeben durch die isolierte Komponente der Zerlegung, die eindeutig bestimmt ist durch die zugehörigen Primideale der Dimensionen $n - 1, \dots, n - i + 1$ und durch dasjenige Primideal von der Dimension $n - i$, dessen Elementarteilerform gleich $P_\lambda^{(i)}$ wird. Zugehörige Primideale und größte primäre Faktoren der Norm entsprechen sich eineindeutig.

Nach § 1, 7. stimmen die r_λ mit ihrem Grundideal i -ter Stufe überein, und besitzen g_{i-1} als Grundideal $(i - 1)$ -ter Stufe; sie lassen also nach Satz VIII bzw. (5) eine kürzeste Darstellung zu: $r_\lambda = [g_{i-1}, q_{\lambda,1}, \dots, q_{\lambda,t_\lambda}]$, wo alle q von der Dimension $n - i$ sind und zu verschiedenen Primidealen gehören. Nach der Definition von $Q_\lambda^{(i)}$ kommt — unter Berücksichtigung, daß r_λ mit seinem Grundideal i -ter Stufe übereinstimmt —:

$$Q_\lambda^{(i)} g_{i-1} \equiv 0 (q_{\lambda,\kappa}); \quad (\kappa = 1, \dots, t_\lambda) \quad \text{und folglich}$$

$$(Q_\lambda^{(i)})^{e_\lambda} \equiv 0 (q_{\lambda,\kappa}); \quad \text{also } (P_\lambda^{(i)})^{e_\lambda e_\lambda} \equiv 0 (p_{\lambda,\kappa}) \quad \text{und somit } P_\lambda^{(i)} \equiv 0 (p_{\lambda,\kappa}),$$

woraus wie beim Beweise von Satz IX folgt, daß in der Darstellung von r_λ nur ein q_λ und zugehöriges p_λ der Dimension $n - i$ auftreten kann; und daß die Elementarteilerform von p_λ durch $P_\lambda^{(i)}$ gegeben ist. Es ist p_λ als zugehöriges Primideal von m nachzuweisen und zu zeigen, daß q_λ in mindestens einer Darstellung von m durch größte primäre Komponenten wirklich auftritt; dann ist damit auch r_λ als isolierte Komponente der Zerlegung erkannt, da kein Primideal in einem von gleicher oder niedrigerer Dimension aufgehen kann und zwar als Komponente, die bestimmt ist durch p_λ und alle zugehörigen Primideale höherer Dimension. Zu diesem Nachweis ist nur zu zeigen, daß q_λ in einer kürzesten Darstellung von g_i auftritt, da sich eine solche nach Satz VIII immer zu einer kürzesten Darstellung von m ergänzen läßt; es ist also nur zu zeigen, daß die Darstellung $g_i = [r_1, \dots, r_a] = [g_{i-1}, q_1, \dots, q_a]$ eine kürzeste wird. Ginge nun etwa q_λ in seinem Komplement auf, wäre also $g_{i-1} q_1 \dots q_{\lambda-1} q_{\lambda+1} \dots q_a$ durch q_λ teilbar, so würde daraus wegen $g_{i-1} \not\equiv 0 (q_\lambda)$ die Teilbarkeit einer Potenz von q_μ durch q_λ folgen für $\mu \neq \lambda$; es würden also, da die zugehörigen Primideale p_μ und p_λ beide gleicher Dimension

sind, diese Primideale nach Satz II übereinstimmen; das ist aber unmöglich, da ihre Elementarteilerformen $P_\mu^{(i)}$ und $P_\lambda^{(i)}$ nach Definition verschieden sind. Die Darstellung von g_i , der nach Satz VIII alle zugehörigen Primideale der Dimension $n - i$ entsprechen, zeigt weiter, daß jedem solchen Primideal auch wirklich ein größter primärer Faktor der Norm entspricht; das eineindeutige Entsprechen ist somit bewiesen.

Satz X ergibt unmittelbar die Übertragung von Satz IV nach

Satz XI. Die einzelnen größten primären Faktoren $Q_\lambda^{(i)} = (P_\lambda^{(i)})^{e_\lambda}$ der Norm lassen eine Produktdarstellung zu:

$$Q_\lambda^{(i)} = \prod (x_i - t_{1i} \bar{y}_{1v} - \dots - t_{ni} \bar{y}_{nv})^{\delta_i e_\lambda} \\ = \prod (t_{1i} (y_1 - \bar{y}_{1v}) + \dots + t_{ni} (y_n - \bar{y}_{nv}))^{\delta_i e_\lambda},$$

wo $\bar{y}_{1v}, \dots, \bar{y}_{nv}$ je ein zusammengehöriges, von $t_{1i}, \dots, t_{ni}$ unabhängiges Nullstellensystem des zugehörigen Primideals p_λ in den ursprünglichen Unbestimmten y darstellt, und δ_i den Wert Eins oder p^{f_i} besitzt; dadurch ist die Zerlegung der Norm in Linearfaktoren vollständig gegeben. Der Grad von $Q_\lambda^{(i)}$ gibt den Grad des durch Restklassen aus g_{i-1} repräsentierten Teiltrings der Restklassen nach der isolierten Komponente r_λ , und zwar in bezug auf den durch Quotientenbildung abgeleiteten Restklassenteilkörper $(P(u, x_{i+1}, \dots, x_n))$; bei primären Idealen handelt es sich also um den Ring aller Restklassen. Bei Adjunktion neuer Unbestimmten v kommt noch die Zerlegung:

$$Q_\lambda^{(i)}(u, v) = \prod (z - v_1 \bar{x}_{1v} - \dots - v_i \bar{x}_{iv})^{\delta_i e_\lambda}.$$

Es handelt sich, da $P_\lambda^{(i)}$ nach Satz X als Elementarteilerform von p_λ erkannt, tatsächlich nur um das Einsetzen der Zerlegung von Satz IV; die Bemerkung über den Grad aber ist nur eine andere Fassung des in § 1, 5. und 7. Gesagten²⁰⁾.

§ 6.

Charakterisierung der Primideale und eigentlichen Primärdeale durch Elementarteilerform und Norm.

In Satz IX waren die Primärdeale durch Elementarteilerform und Norm charakterisiert, aber nur in der Art, daß prim als Spezialfall von

²⁰⁾ Ebenso ist auch die in Anm. ²⁾ von H.-N. erwähnte Fassung der Multiplizität eine unmittelbare Folge von Satz X. Denn das Restklassensystem $g_{i-1} | r_\lambda$ ist — bei Adjunktion von $x_{i+1}, \dots, x_n$ — isomorph zu $t_\lambda | r_\lambda$, wo $t_\lambda = [g_{i-1}, r_1, \dots, r_{\lambda-1}, r_{\lambda+1}, \dots, r_\alpha]$ gesetzt ist, wie das Zurückgehen auf Moduln aus Linearformen (H.-N., Satz V) in Betracht der Teilerfremdheit der $Q_\mu^{(i)}$ unmittelbar zeigt; $t_\lambda | r_\lambda$ wird isomorph zu $t_\lambda | q_\lambda$. Dabei entsteht t_λ aus dem Komplement von q_λ bei Adjunktion von $x_{i+1}, \dots, x_n$. δ_i ist die Multiplizität von q_λ in g_i .

primär zu betrachten war. Es handelt sich jetzt um die Trennung von Primidealen und eigentlichen Primäridealen; die Überlegungen werden denen von § 3 parallel laufen. Bedingungen, die entweder notwendig oder hinreichend sind, lassen sich leicht angeben nach

Satz XII. *Eine notwendige Bedingung für ein Primideal ist, daß die Elementarteilerform Primfunktion ist, eine hinreichende, daß die Norm Primfunktion ist. M. a. W. die Elementarteilerform eines Primideals ist stets eine Primfunktion, die Norm eines eigentlichen Primärideals stets eine eigentliche Primärfunktion.*

Daß die Elementarteilerform eines Primideals eine Primfunktion wird, war schon in Satz I gezeigt. Sei jetzt die Norm R_q gleich einer Primfunktion; es ist zu zeigen, daß bei dieser Voraussetzung jeder echte Teiler a von q von niedrigerer Höchstdimension wird, wodurch q nach Satz II als Primideal erkannt ist. In der Tat wird nach § 1, 6. der erste Faktor der Norm R_a , der von dem entsprechenden von R_q verschieden ist, ein echter Teiler; wegen $R_q = P^{(i)}$ muß somit der Faktor $R^{(i)}$ von R_a gleich einem echten Teiler von $P^{(i)}$, also gleich der Einheit werden; a wird von niedrigerer Höchstdimension.

Ein zweiter einfacher Beweis beruht auf dem auch dem folgenden Satz zugrunde liegenden

Hilfssatz VII. *Das durch Polynome $H^{(i)}$ repräsentierte System der Restklassen nach der Elementarteilerform $E^{(i)}$ eines Primärideals — allgemeiner eines Ideals, das nur zugehörige Primideale der Dimension $n - i$ besitzt — ist isomorph einem Teilsystem der Restklassen nach diesem Ideal. Der Grad der Elementarteilerform gibt den Grad dieses Restklassensystems in bezug auf den Quotientenkörper $(P(u, x_{i+1}, \dots, x_n))$ an.*

In der Tat läßt sich eine Zuordnung herstellen dadurch, daß die durch gleiche Polynome $H^{(i)}$ repräsentierten Klassen einander zugeordnet werden; Summe und Produkt entsprechen dabei Summe und Produkt. Die Zuordnung ist aber auch eineindeutig; denn alle der Nullklasse nach dem Ideal angehörenden Polynome $H^{(i)}$ sind nach Definition durch $E^{(i)}$ teilbar; der Nullklasse entspricht also die Nullklasse nach $E^{(i)}$, und natürlich gilt auch das Umgekehrte.

Sei jetzt die Norm eines Ideals eine Primfunktion $P^{(i)}$, also mit der Elementarteilerform identisch. Folglich stimmen die Grade der Restklassensysteme nach der Elementarteilerform $P^{(i)}$ und nach q in bezug auf $(P(u, x_{i+1}, \dots, x_n))$ überein; das dem Restklassensystem nach $P^{(i)}$ isomorphe Teilsystem erschöpft also die Restklassen nach q ; und da dies System keine Nullteiler besitzen kann, wird q Primideal.

Wenn a ein echter Teiler von q ist, so ist $R_a \neq R_q$, was nach Satz I folgt.

Im allgemeinen läßt Satz XII sich nicht zu notwendigen und hinreichenden Bedingungen verschärfen, wie weiter unten an Beispielen gezeigt werden wird. Dagegen ist dies der Fall, wenn der Koeffizientenbereich P ein vollkommener Körper (§ 1, 14.) ist, nach

Satz XIII. *Ist der Koeffizientenbereich P ein vollkommener Körper, so werden Norm und Elementarteilerform eines Primideals Primfunktionen und folglich identisch, Norm und Elementarteilerform eines eigentlichen Primärideals eigentliche Primärfunktionen. Die Bedingung, daß die Elementarteilerform Primfunktion ist, ist also bei vollkommenem Körper eine notwendige und hinreichende für ein Primideal; statt der Elementarteilerform kann in der Bedingung auch die Norm stehen.*

Unter Berücksichtigung von Satz XII wird Satz XIII bewiesen sein, wenn gezeigt ist, daß bei vollkommenem Körper das Ideal Primideal wird, sobald die Elementarteilerform Primfunktion ist; und daß dann die Norm gleich dieser Primfunktion wird. Nun war in Hilfssatz V, § 3 gezeigt, daß bei vollkommenem Körper die Elementarteilerform eine Primfunktion *erster Art* wird, sobald sie überhaupt Primfunktion ist. Bedeutet daher $(\mathfrak{R})$ den durch Adjunktion von (x_i) zu $(P(u, x_{i+1}, \dots, x_n))$ entstandenen Restklassenkörper $(P(u, x_i, x_{i+1}, \dots, x_n))$ nach $P^{(i)}$, so wird (x_i) Nullstelle der Primfunktion erster Art $(P^{(i)})$, und folglich sind, wie etwa die Lagrangesche Formel zeigt, $(y_1), \dots, (y_n)$ in $(\mathfrak{R})$ enthalten. Das nach Hilfssatz VII zu $(\mathfrak{R})$ isomorphe Teilsystem der Restklassen nach dem betrachteten Ideal q — wobei es sich nur um Auftreten von Nennern aus $(P(u, x_{i+1}, \dots, x_n))$ handelt — enthält also die Restklassen $(y_1), \dots, (y_n)$ und erschöpft folglich das Restklassensystem nach q ; da es aber als zu $(\mathfrak{R})$ isomorph keine Nullteiler besitzen kann, wird q Primideal. Der Grad dieses Restklassenkörpers $(\mathfrak{R})$ von q in bezug auf $(P(u, x_{i+1}, \dots, x_n))$ wird gleich dem Grad der Norm von q ; andererseits wegen des Isomorphismus zu $(\mathfrak{R})$ gleich dem Grad der Elementarteilerform $P^{(i)}$; somit müssen Norm und Elementarteilerform übereinstimmen.

Bei unvollkommenem Körper läßt Satz XII immerhin noch die Verschärfung zu:

Satz XIV. *Ist der Koeffizientenbereich P ein unvollkommener Körper von der Charakteristik p , so wird die Norm eines Primideals die p^g -te Potenz der Elementarteilerform; es wird $0 \leq g \leq (i-1)f$, wo f den Exponenten der Elementarteilerform, $n-i$ die Dimension des Primideals bedeutet.*

Satz XIV kommt auf die Behauptung hinaus, daß der Restklassenkörper $(\mathfrak{R})$ von p vom Grade p^g ($g \geq 0$) in bezug auf den zu $(\mathfrak{R})$ isomorphen Teilkörper $(\mathfrak{R}') = (P(u, x_i, x_{i+1}, \dots, x_n))$ wird. Das wird aber

unmittelbar aus den in § 1, 15. angegebenen Steinitz'schen Sätzen folgen, genauer aus

Hilfssatz VIII. *Ist $\mathfrak{L}$ eine endliche Erweiterung des unvollkommenen Körpers Ω vom reduzierten Grade r und Exponenten f , $\mathfrak{L}_0$ der in $\mathfrak{L}$ enthaltene Körper erster Art, $\mathfrak{M}$ ein Zwischenkörper von $\mathfrak{L}_0$ und $\mathfrak{L}$, so wird der Grad jedes Elementes aus $\mathfrak{L}$ in bezug auf $\mathfrak{M}$ eine Potenz von p , wo p die Charakteristik von Ω bedeutet.*

Denn es gehört die $p^{f'}$ -te Potenz ($f' \leq f$) jedes Elementes z aus $\mathfrak{L}$ zu $\mathfrak{L}_0$; somit wird z Nullstelle einer Primfunktion $G(t) = (t - z)^{p^{f'}}$ mit Koeffizienten aus $\mathfrak{L}_0$. Sei $H(t) = (t - z)^{\delta}$ die Primfunktion in $\mathfrak{M}$ mit der Nullstelle z ; dann hat $H(t)$ auch Koeffizienten aus $\mathfrak{L}_0(z)$ und somit gehören die Koeffizienten von $H(t)$ dem Durchschnittskörper von $\mathfrak{M}$ und $\mathfrak{L}_0(z)$ an, also einem Zwischenkörper von $\mathfrak{L}_0$ und $\mathfrak{L}_0(z)$. Der Grad von z in bezug auf $\mathfrak{M}$ wird also gleich dem Grad in bezug auf diesen Zwischenkörper, somit als Teiler von $p^{f'}$ eine Potenz von p .

Zum Beweise von Satz XIV ist jetzt nur zu bemerken, daß der Körper $(\mathfrak{R}') = (P(u, x_i, x_{i+1}, \dots, x_n))$ vom Grade $r \cdot p^f$ in bezug auf $(P(u, x_{i+1}, \dots, x_n))$ sein muß, wenn r den reduzierten Grad, f den Exponenten von $(\mathfrak{R})$ bedeutet; und daß folglich der in $(\mathfrak{R})$ enthaltene Körper erster Art $(\mathfrak{R}_0)$ Teilkörper von $(\mathfrak{R}')$ sein muß. Denn da es Elemente vom Grade $r \cdot p^f$ in $(\mathfrak{R})$ gibt (§ 1, 15.), muß notwendig (x_i) von diesem Grad sein, da alle Elemente aus $(\mathfrak{R})$ durch Spezialisierung der $t_{\mu r}$ in (x_i) entstehen; der Exponent von $(\mathfrak{R})$ stimmt also mit dem Exponenten der Elementarteilerform überein und $(x_i)^{p^f}$ wird vom Grade r und Element von $(\mathfrak{R}_0)$, somit primitives Element von $(\mathfrak{R}_0)$. Da aber $(\mathfrak{R})$ durch Adjunktion endlichvieler Elemente — etwa $(x_1), \dots, (x_{i-1})$ — zu $(\mathfrak{R}')$ entsteht, ergibt die endlich oftmalige Anwendung von Hilfssatz VIII den gewünschten Beweis und zugleich die Abschätzung für g .²¹⁾

Es seien jetzt noch die Beispiele nachgetragen, die zeigen, daß Satz XII sich im allgemeinen nicht über Satz XIV hinaus verschärfen läßt; es handelt sich um ein Primideal, dessen Norm gleich dem Quadrat der Elementarteilerform wird ($g > 0$), und um eigentliche Primärdeale, deren Elementarteilerform Primfunktionen werden; letzteres Beispiel zeigt zugleich, daß hier kein Analogon zu Satz XIV besteht, sondern daß die Norm eine beliebige Potenz der Elementarteilerform werden kann.

Der Koeffizientenbereich P entstehe durch Adjunktion zweier Unbestimmten λ, μ zu dem Körper der Restklassen modulo 2, sei also ein

²¹⁾ Vgl. hierzu die parallel laufenden Überlegungen bei A. Ostrowski, Zur arithmetischen Theorie der algebraischen Größen, Gött. Nachr. 1919, S. 279–298; insbesondere S. 288, wo der entsprechende Satz ohne Beweis ausgesprochen ist.

Handwritten note: $\mathfrak{L} = \mathfrak{L}_0(z)$ mit $z \in \mathfrak{L}$

unvollkommener Körper von der Charakteristik zwei. Es handle sich um das Ideal $\bar{p} = (y_1^2 + \lambda, y_2^2 + \mu)$, das Primideal sein muß, da das Restklassensystem $(\bar{R})$ dem Körper $P(\sqrt{\lambda}, \sqrt{\mu})$ isomorph wird. $(\bar{R})$ wird vom vierten Grad in bezug auf $(\bar{P})$, vom reduzierten Grad $r=1$, vom Exponenten $f=2$; die Elementarteilerform $P^{(2)}$ wird also zweiten Grades, die Norm vierten Grades und somit Quadrat von $P^{(2)}$, wie auch die Modularstellung (3), § 1, 5. leicht nachrechnen läßt; es kommt $P^{(2)} = (u_{11}u_{22} + u_{12}u_{21})^2 x_2^2 + (u_{11}^2\mu + u_{21}^2\lambda)$ oder auch nach geeigneter Multiplikation: $x_2^2 + (t_{12}^2\lambda + t_{22}^2\mu)$.

Es entstehe jetzt P durch Adjunktion der einen Unbestimmten λ zu dem Körper der Restklassen modulo 2, und es werde das Ideal $\bar{q} = (y_1^2 + \lambda, y_2^2 + \lambda) = (y_1^2 + \lambda, (y_1 + y_2)^2)$ zugrunde gelegt. Als Elementarteilerform kommt durch die Spezialisierung $\mu = \lambda$ aus der oben angegebenen: $P^{(2)} = x_2^2 + \lambda(t_{12}^2 + t_{22}^2)$, also eine Primfunktion, da $t_{12} = (0)$, $t_{22} = (1)$ zu der Primfunktion $x_2^2 + \lambda$ führt. $\bar{q}$ wird aber eigentlich primär, da es $(y_1 + y_2)^2$, aber nicht $(y_1 + y_2)$ enthält. Die Norm muß gleich dem Quadrat, also gleich der p -ten Potenz, von $P^{(2)}$ werden, da die Anzahl der in bezug auf P linear unabhängigen Restklassen von $\bar{q}$ gleich vier beträgt.

Daß dies letztere Analogon zu Satz XIV nicht immer erfüllt ist, zeige folgendes Beispiel: P entstehe durch Adjunktion der Unbestimmten λ zu dem Restklassenkörper modulo 3; es werde $\bar{q} = (y_1^3 + \lambda, (y_1 - y_2)^3)$ zugrunde gelegt, so daß es sich also wie oben um ein eigentliches Primärideal handelt. Die Elementarteilerform wird — unter Berücksichtigung, daß auch $y_2^3 + \lambda$ durch $\bar{q}$ teilbar — gleich $P^{(2)} = x_2^3 + \lambda(t_{12}^3 + t_{22}^3)$, also Primfunktion; die Norm wird aber gleich dem Quadrat von $P^{(2)}$, da es sich um sechs linear unabhängige Restklassen nach $\bar{q}$ handelt. Es tritt hier also nicht die p -te Potenz der Elementarteilerform auf.

Das erste Beispiel zeigt, daß bei unvollkommenem Körper als Koeffizientenbereich genau wie in algebraischen Zahlkörpern Primideale von höherem als dem ersten Grad auftreten können, wo p^g als Grad des Primideals zu bezeichnen ist. Die weiteren Beispiele sind als Analogon zu Verzweigungsideal aufzufassen, also dazu, daß eine Primzahl durch eine höhere Potenz eines Primideals, durch ein Primärideal teilbar wird; denn wie in Anmerkung ¹⁰⁾ gezeigt, entspricht die Elementarteilerform der kleinsten ganzen rationalen Zahl, die durch ein Ideal in einem algebraischen Zahlkörper teilbar wird.

§ 7.

Absolute Primideale.

Ein Primideal mit Koeffizienten aus P wird als *absolutes Primideal* bezeichnet, wenn es Primideal bleibt in dem algebraisch abgeschlossenen

in P ist und Primideal.

Körper A ; zu dem P sich erweitern läßt²²⁾). Entsprechend heißt eine Primfunktion P mit Koeffizienten aus P *absolute Primfunktion* — *absolut irreduzibles Polynom* —, wenn P Primfunktion in A bleibt. Die Charakterisierung der absoluten Primideale wird geleistet durch

Satz XV. *Eine notwendige und hinreichende Bedingung für ein absolutes Primideal besteht darin, daß seine Elementarteilerform — die als ganz und primitiv in den u vorausgesetzt werden darf — eine absolute Primfunktion als Polynom der x und u wird. Die Elementarteilerform wird mit der Norm identisch, so daß die Bedingung sich auch für die Norm aussprechen läßt.*

Zum Beweise ist vorerst zu bemerken, daß allgemein Norm und Elementarteilerform bei algebraischer Erweiterung des Koeffizientenbereichs erhalten bleiben. Denn die einzelnen Faktoren $R^{(i)}$ bzw. $E^{(i)}$ sind definiert als größte gemeinsame Teiler im Polynomsinn, eine Eigenschaft, die bei algebraischer Erweiterung des Koeffizientenbereichs erhalten bleibt. Es bleibt also $P^{(i)}$ auch Elementarteilerform von p beim Übergang von P zu A , also beim Übergang zu einem vollkommenen Körper als Koeffizientenbereich; denn jeder algebraisch abgeschlossene Körper ist vollkommen, wie die Definition unmittelbar zeigt. Nach Satz XIII ist daher eine notwendige und hinreichende Bedingung für p als absolutes Primideal, daß $P^{(i)}$ Primfunktion in bezug auf $A(u)$ wird; also absolute Primfunktion als Polynom der x und u , wenn $P^{(i)}$ als ganz und primitiv in den u vorausgesetzt wird. Zugleich wird $P^{(i)}$ nach Satz XIII auch mit der Norm von p identisch, sobald A als Koeffizientenbereich zugrunde gelegt wird; also gilt nach dem oben Bemerkten das gleiche auch bei Zugrundelegung von P , womit Satz XV bewiesen ist.

Für *absolute Primfunktionen* P mit Koeffizienten aus einem (endlichen) algebraischen Zahlkörper $\mathfrak{K}$ gilt nun der Satz²³⁾, daß P *Primfunktion bleibt, genauer absolute Primfunktion modulo jedes Primideals aus $\mathfrak{K}$, höchstens mit Ausnahme von endlich vielen Primidealen aus $\mathfrak{K}$* . Die Übertragung dieses Satzes auf absolute Primideale stützt sich auf

Satz XVI. *Wird als Koeffizientenbereich an Stelle eines Körpers der Ring $\mathfrak{o}^*$ aller ganzen algebraischen Zahlen eines (endlichen) algebraischen Zahlkörpers $\mathfrak{K}$ zugrunde gelegt, so bleibt Norm und Elementarteilerform eines*

²²⁾ Ein algebraisch abgeschlossener Körper ist bekanntlich ein solcher, in dem jedes Polynom einer Unbestimmten in Linearfaktoren zerfällt. Existenz und wesentliche Eindeutigkeit des zu einem beliebigen Körper gehörenden algebraisch abgeschlossenen Körpers bei Steinitz.

²³⁾ A. Ostrowski: a. a. O. (Anm. ²¹⁾); Hilfssatz S. 296. — Einfacherer Beweis bei E. Noether, Ein algebraisches Kriterium für absolute Irreduzibilität, Math. Ann. 85 (1922), S. 26–33, Nr. 7.

Polynomideals als Norm und Elementarteilerform erhalten modulo jedes Primideals aus $\mathfrak{R}$, höchstens mit Ausnahme von endlich vielen Primidealen aus $\mathfrak{R}$.

Zum Beweise ist der zugrunde gelegte Polynombereich gegenüber § 1, 1. zu modifizieren. Es bestehe $\mathfrak{S}$ aus allen Polynomen in $y_1, \dots, y_n$ mit Koeffizienten aus $\mathfrak{o}^*$, also ganzen algebraischen Zahlen aus $\mathfrak{R}$; der Koeffizientenbereich von $\mathfrak{S}$ sei $\mathfrak{o}^*[u]$, d. h. alle Polynome in u mit Koeffizienten aus $\mathfrak{o}^*$. Ist $\bar{m}$ ein Ideal in $\mathfrak{S}$, so geht es vermöge (1) in ein transformiertes Ideal m in $\mathfrak{S}$ über. Es ist nachzuweisen, daß zur Bildung der Norm nur eine endliche Anzahl von Polynomen aus $\mathfrak{o}^*[u]$ im Nenner auftritt, woraus Satz XVI direkt folgen wird.

Dazu ist vorerst zu bemerken, daß die Moduldarstellung (3) in § 1, 5. zur Bildung der Einzelnorm hinauskommt auf eine Reduktion der Potenzen von x_{i-1} modulo einem in x_{i-1} regulären Polynom $C^{(i-1)} = U_{i-1}(u)x_{i-1}^i + \text{niedrigere Glieder}^{24)}$; dabei dürfen alle Koeffizienten von $C^{(i-1)}$, insbesondere also U_{i-1} , als Größen aus $\mathfrak{o}^*[u]$ angenommen werden. Da es sich um sukzessive Reduktion von $x_1, \dots, x_{i-1}$ handelt, wird also die in den x ganze Moduldarstellung auch ganz in $\mathfrak{o}^*[u]$ bis auf Potenzprodukte $U_1^{\lambda_1} \dots U_{i-1}^{\lambda_{i-1}}$ im Nenner. Das Produkt $U_1 U_2 \dots U_n$, aufgefaßt als Polynom in den u , definiert aber durch seine Koeffizienten ein Ideal $\mathfrak{r}^*$ aus $\mathfrak{R}$, das mithin nur durch endlich viele Primideale aus $\mathfrak{R}$ teilbar wird. Nimmt man $\mathfrak{p}^*$ verschieden von diesen endlich vielen an, und legt als Koeffizientenbereich den Restklassenkörper nach $\mathfrak{p}^*$ zugrunde, so bleibt also die ursprüngliche Moduldarstellung erhalten, indem nur jede Zahl aus $\mathfrak{o}^*$ durch ihre Restklasse nach $\mathfrak{p}^*$ ersetzt wird.

Es lassen sich ferner Norm und Elementarteilerform, da sie nur bis auf Faktoren aus $\mathfrak{o}^*[u]$ bestimmt sind, auch in bezug auf $\mathfrak{o}^*[u]$ durch m teilbar annehmen. Sei bei dieser Annahme etwa $R^{(i)} = V_i(u)x_i^i + \text{niedrigere Glieder}$, so daß bei der Teilbarkeit aller ϱ -reihigen Determinanten des durch $C^{(i-1)}$ bestimmten Moduls $\mathfrak{M}_{i-1}^*$ vom Rang ϱ nur Potenzen von V_i außer den $U_1^{\lambda_1} \dots U_{i-1}^{\lambda_{i-1}}$ im Nenner auftreten. Wählt man daher $\mathfrak{p}^*$ auch noch verschieden von den endlich vielen Primidealen aus $\mathfrak{R}$, die in dem durch $V_1 V_2 \dots V_n$ bestimmten Ideal aus $\mathfrak{R}$ aufgehen, so bleibt $R^{(i)}$ gemeinsamer Teiler dieser Determinanten bei Zugrundelegung des Restklassenkörpers nach $\mathfrak{p}^*$ als Koeffizientenbereich und der Rang von $\mathfrak{M}_{i-1}^*$ bleibt erhalten, da $C^{(i)}$ eine ϱ -reihige Determinante aus $\mathfrak{M}_{i-1}^*$ war. Schließlich ist $\mathfrak{p}^*$ noch so zu wählen, daß $R^{(i)}$ jeweils größter gemeinsamer Teiler bleibt. Es durchlaufe $D^{(i)}$ alle ϱ -reihigen Determinanten aus $\mathfrak{M}_{i-1}^*$, so daß nach Voraussetzung $U_1^{\lambda_1} \dots U_{i-1}^{\lambda_{i-1}} V_i^\sigma D^{(i)} = R^{(i)} T^{(i)}$ kommt, wo also

²⁴⁾ Vgl. dazu H.-N. § 4.

die $T^{(i)}$ keinen gemeinsamen, x enthaltenden Teiler im Polynomsinn besitzen. Folglich enthält das aus allen $T^{(i)}$ abgeleitete Ideal ein Polynom $G^{(i+1)} = W_i(u)x_{i+1}^m + \text{niedrigere Glieder}$, $W_i \neq 0$; daß dabei $G^{(i+1)}$ als regulär in x_{i+1} angenommen werden darf, zeigt die Zusammensetzung der Transformation (1) mit einer solchen von $x_{i+1}, \dots, x_n$ mit neuen Unbestimmten als Koeffizienten. Wählt man also $\mathfrak{p}^*$ auch noch verschieden von den endlich vielen Primidealen, die in dem durch $W_1 W_2 \dots W_n$ bestimmten Ideal aus $\mathfrak{R}$ aufgehen, so bleibt bei Zugrundelegung des Restklassenkörpers nach $\mathfrak{p}^*$ als Koeffizientenbereich tatsächlich R_m als Norm erhalten. Ganz entsprechend läßt sich $\mathfrak{p}^*$ weiter noch so wählen, daß auch E_m als Elementarteilerform erhalten bleibt; Satz XVI ist damit bewiesen.

Aus Satz XV und XVI folgt als *Verallgemeinerung des Satzes über die absoluten Primfunktionen* und unter Benutzung dieses Satzes

Satz XVII. *Ist $\mathfrak{p}$ ein absolutes Primideal mit ganzen Zahlen aus einem (endlichen) algebraischen Zahlkörper $\mathfrak{R}$ als Koeffizienten, so bleibt $\mathfrak{p}$ Primideal, genauer absolutes Primideal modulo jedes Primideals aus $\mathfrak{R}$, höchstens mit Ausnahme von endlich vielen Primidealen aus $\mathfrak{R}$.*

Zum Beweise sei die Norm R_p von $\mathfrak{p}$ wie in Satz XVI so gewählt, daß sie auch in bezug auf $\mathfrak{o}^*[u]$ durch $\mathfrak{p}$ teilbar wird; es wird dann $R_p = T(u)P^{(i)}(x)$, wo $P^{(i)}(x)$ als ganz und primitiv in den u angenommen werden darf. $P^{(i)}$ wird folglich nach Satz XV, aufgefaßt als Polynom in u und x mit Koeffizienten aus $\mathfrak{R}$, eine absolute Primfunktion. Nach dem Satz über die absoluten Primfunktionen behält $P^{(i)}$ diese Eigenschaft modulo jedes Primideals aus $\mathfrak{R}$, höchstens mit Ausnahme von endlich vielen Primidealen aus $\mathfrak{R}$. Wählt man also $\mathfrak{p}^*$ verschieden von diesen endlich vielen Primidealen, und nach Satz XVI noch verschieden von endlich vielen weiteren Primidealen aus $\mathfrak{R}$, so wird $P^{(i)}$ — dessen Koeffizienten aus $\mathfrak{o}^*$ durch die entsprechenden Restklassen nach $\mathfrak{p}^*$ zu ersetzen sind — Norm von $\mathfrak{p}$ bei Zugrundelegung des Restklassenkörpers nach $\mathfrak{p}^*$ als Koeffizientenbereich P , und diese Norm wird absolute Primfunktion. Bei Zugrundelegung von P als Koeffizientenbereich bleibt also $\mathfrak{p}$ nach Satz XV absolutes Primideal, womit Satz XVII bewiesen ist.

Göttingen, 8. Mai 1923.

(Eingegangen am 9. 3. 1923.)