Algebraische Theorie der zerlegbaren Ringe.

(Algebraische Theorie der Ringe. III.)

Von

Wolfgang Krull in Freiburg i. Br.

Die vorliegende Arbeit soll eine Fortführung und Ergänzung der Abhandlungen „Algebraische Theorie der Ringe I und II“[1]) darstellen. Dort wurde für eine gewisse Klasse von Ringen, die im wesentlichen endliche oder unendliche Systeme hyperkomplexer Größen mit kommutativer Multiplikation sind, der Begriff der algebraischen und transzendenten Erweiterung nach dem Vorbild der Körpertheorie eingeführt. Mit Hilfe der Übertragung der körpertheoretischen Methoden gelangt man dann zu einer *Typisierung* der betrachteten Ringe, wenigstens der vollkommenen, die dadurch ausgezeichnet sind, daß ihnen ein vollkommener Körper zugeordnet werden kann.

Im folgenden soll nun untersucht werden, wie die Verhältnisse, insbesondere die Fragen der Typisierung, in einem gewissen ausgezeichneten Falle, nämlich bei den sogenannten zerlegbaren Ringen, liegen. Der Begriff des zerlegbaren Ringes wurde von Herrn Fraenkel in seiner Dissertation[2]) axiomatisch festgelegt. Die zerlegbaren Ringe sind dadurch gekennzeichnet, daß sich in ihnen die Null im wesentlichen eindeutig als Produkt von Potenzen von „Primteilern“ (der Null) darstellen läßt. Axiomatisch kann man sie, wie in § 1 der vorliegenden Arbeit gezeigt wird, auch charakterisieren als *„Ringe, in denen es nur Nullteiler und Einheiten gibt, und in denen außerdem jedes Ideal ein Hauptideal ist, also aus der Gesamtheit aller durch ein festes Element teilbaren Ringelemente*

---

[1]) Math. Annalen **88**, S. 80–122, bzw. Math. Annalen **91**, S. 1–46. Diese Arbeiten werden in Zukunft mit A. I und A. II zitiert.

[2]) „Über die Teiler der Null und Zerlegung von Ringen“. Journal f. Math. **145**, S. 139–176. Diese Arbeit wird im folgenden mit „F.“ zitiert. Ferner wollen wir unter „N.“ die Arbeit „Idealtheorie in Ringbereichen“, Math. Annalen **83**, S. 24–67 von E. Noether verstehen.

besteht". Nach den allgemeinen Ergebnissen von A. II bzw. nach den Resultaten der Fraenkelschen Dissertation läßt sich jeder zerlegbare Ring als Summe von endlich vielen speziellen Ringen darstellen, wobei ein spezieller Ring dadurch ausgezeichnet ist, daß in ihm sich jeder Nullteiler als Produkt einer eindeutig bestimmten Potenz eines ein für allemal festgelegten Primteilers mit einer Einheit darstellen läßt. Wir hatten bereits in A. II mit einer ausgezeichneten Klasse von speziellen zerlegbaren Ringen, nämlich mit den sogenannten „Grundringen" zu tun. Im folgenden beschäftigen wir uns genau wie in den vorangehenden Arbeiten vorwiegend mit Ringen des speziellen Typs.

Zunächst werden die Vereinfachungen dargelegt, die sich hinsichtlich der Theorie der algebraischen und transzendenten Erweiterungen bei den zerlegbaren Ringen gegenüber dem allgemeinen Fall ergeben. Die leicht zugängliche Natur der zerlegbaren Ringe zeigt sich u. a. darin, daß wir den Aufbau der Polynomideale einer Variablen besser übersehen können als im allgemeinen Fall, und daß sich insbesondere für jedes Polynomideal eine Normalbasis einfacher Art aufstellen läßt. Des ferneren lassen sich, wie in § 3 gezeigt wird, die regulären Erweiterungen eingehender charakterisieren als im allgemeinen Fall und zwar durch den wichtigen Satz:

Die regulären Erweiterungen eines zerlegbaren speziellen Ringes sind die einzigen Erweiterungen, die wieder zu einem speziellen zerlegbaren Ring mit dem gleichen charakteristischen Exponenten führen.

Die Bedeutung dieses Theorems zeigt sich u. a. bei der Typisierung der vollkommenen Ringe. Man kann z. B. mit Hilfe unseres Satzes unmittelbar einsehen, daß die vollkommenen Grundringe die einzigen vollkommenen speziellen zerlegbaren Ringe sind, die den gleichen charakteristischen Exponenten wie ihr Primring besitzen.

Von besonderer Wichtigkeit ist bei der Typisierung noch eine weitere Untersuchung, die nur bei zerlegbaren Ringen durchführbar ist. Im allgemeinen Fall mußten wir uns, um zu befriedigenden Ergebnissen zu gelangen, auf „reguläre" Erweiterungen beschränken, durch die dem gegebenen Ring nach einer in A. II verwandten Ausdrucksweise gleichsam nur reguläre Elemente zugefügt werden. *Bei zerlegbaren Ringen beschäftigen wir uns auch mit allgemeinen algebraischen Erweiterungen, durch die neue Nullteiler eingeführt werden, und zwar mit solchen, die einen zerlegbaren Ring wieder in einen zerlegbaren verwandeln.* Es gelingt, derartige Erweiterungen erschöpfend zu charakterisieren, und einen genauen Einblick in ihren Aufbau zu gewinnen.

Aus dem gewonnenen Resultat ergeben sich wichtige Folgerungen für die *Typisierung der zerlegbaren Ringe.* Zunächst gewinnen wir mit Hilfe der allgemeinen algebraischen Erweiterungen einen befriedigenden Einblick in die Natur der *endlichen zerlegbaren Ringe,* und zwar zeigt es sich, daß man für alle hier in Betracht kommenden Typen Beispiele gewinnen kann, wenn man Restklassensysteme nach geeignet gewählten Idealen aus algebraischen Zahlkörpern betrachtet. Allerdings ist damit noch nicht bewiesen, daß jeder endliche zerlegbare Ring dem Restklassensystem eines algebraischen Ideales isomorph ist. Um diese Frage beantworten zu können, müßte man, wie im Texte dargelegt wird, jedenfalls erst über eine Reihe von Existenzsätzen aus der algebraischen Zahlentheorie Bescheid wissen.

Ähnlich wie bei den endlichen liegen die Verhältnisse bei beliebigen *vollkommenen zerlegbaren Ringen.* Auch hier gelangen wir auf Grund der Tatsache, daß *jeder vollkommene zerlegbare Ring aus seinem Grundring durch allgemeine algebraische Erweiterung entsteht,* zu einer genauen Charakterisierung der untersuchten Bereiche. *Besonders interessant sind die Verhältnisse bei den algebraisch abgeschlossenen zerlegbaren Ringen. Hier gelingt es uns nämlich, notwendige und hinreichende Kennzeichen dafür zu gewinnen, wann ein solcher Ring durch Grundring und charakteristischen Exponenten eindeutig bestimmt ist und wann nicht.* Dabei zeigt sich eine neue beachtenswerte Analogie mit der Körpertheorie: Der Unterschied zwischen den durch Grundring und charakteristischen Exponenten eindeutig bestimmten Ringen und den andern ist ganz ähnlich dem Unterschied zwischen vollkommenen und unvollkommenen Körpern (obwohl alle hier in Betracht kommenden Ringe in unserer in A. I und A. II eingeführten Ausdrucksweise vollkommen sind) — die Primteiler der Null spielen eine analoge Rolle wie die transzendenten Elemente in der Körpertheorie.

Außer diesen neuen Beziehungen zur Körpertheorie ergibt sich bei den zuletzt besprochenen Untersuchungen noch eine Reihe merkwürdiger Fragen, so daß es scheint, als ob die hier entwickelte algebraische Behandlungsweise nicht nur hinsichtlich der Typisierung der zerlegbaren Ringe zu einem gewissen Abschluß führte, sondern auch den geeigneten Ausgangspunkt zu einer weiteren Untersuchung dieser Bereiche böte.

§ 1.

Die allgemeinen zerlegbaren Ringe.

Ein allgemeiner zerlegbarer Ring ist ein Ringbereich mit kommutativer Multiplikation und universellem Einheitselement[3]) r_ε, der folgenden Axiomen genügt:

---

[3]) Zu der Definition des allgemeinsten kommutativen Ringbereichs vgl. A. I § 1.

I. *Ein Element a aus R ist entweder Nullteiler oder Einheit, d. h. es besteht stets entweder eine Gleichung* $a \cdot \bar{a} = 0$; $\bar{a} \neq 0$ *oder eine Gleichung* $a \cdot a^{-1} = r_\varepsilon$.

II. *Jedes Ideal aus R ist ein Hauptideal* (a), *besteht also aus der Gesamtheit der durch ein festes Element a teilbaren Ringelemente.*

Auf Grund dieser beiden Axiome beweisen wir zunächst folgenden Satz[4]):

Hilfssatz 1. *Besitzt das Ideal* $\mathfrak{a} = (a)$ *einen vom Einheitsideal* $\mathfrak{o}$ *verschiedenen echten Teiler* $\mathfrak{b} = (b)$, *so läßt es sich auch als Produkt echter Teiler darstellen.*

Da die Ideale $\mathfrak{a}$ und $\mathfrak{b}$ vom Einheitsideal verschieden sind, so müssen infolge von Axiom I die Elemente a und b Nullteiler sein, und wegen der Teilbarkeit von $\mathfrak{a}$ durch $\mathfrak{b}$ muß eine Gleichung $a = b \cdot c$ bestehen, aus der dann die Idealgleichung $(a) = (b) \cdot (c)$ folgt. Sollte nun (c) ein echter Teiler von $\mathfrak{a}$ sein, so ist unsere Behauptung bewiesen, im andern Falle muß jedenfalls eine Gleichung $c = d \cdot a$ bestehen. Ist dann $\bar{b} \neq 0$ ein nach Vor. existierendes Element, das der Gleichung $b \cdot \bar{b} = 0$ genügt, so kann $\bar{b}$ und folglich auch $\bar{b} + d \cdot a = \bar{b} + c$ nicht durch a teilbar sein, weil sonst entgegen der Wahl von $\bar{b}$ die Gleichung $\bar{b} = e \cdot a = e \cdot b \cdot c = e \cdot a \cdot b \cdot d = \bar{b} \cdot b \cdot d = 0$ bestände. Die Ideale $(\bar{b} + c)$ und $\mathfrak{a}$ sind mithin verschieden, und aus der Gleichung $\mathfrak{a} = (\bar{b} + c) \cdot (b)$ folgt die Behauptung des Hilfssatzes.

Da ein Primideal seiner Definition gemäß nicht als das Produkt von echten Teilern darstellbar ist, so folgt aus dem gewonnenen Ergebnis unmittelbar, daß in R kein Primideal einen von $\mathfrak{o}$ verschiedenen echten Teiler besitzen kann. Daraus ergibt sich weiter, daß *die zerlegbaren Ringe dem allgemeinen in* A. II § 1 *u.* § 2 *charakterisierten Ringtypus angehören*, und wir können aus A. II die folgenden Sätze übernehmen, die sich für zerlegbare Ringe mit Benutzung von Hilfssatz 1 auch direkt beweisen lassen:

Jeder allgemeine zerlegbare Ring läßt sich als eindeutige Summe von endlich viel speziellen Ringen, in denen die Gesamtheit der Nullteiler ein Primideal bildet, darstellen[5]).

Ist $\mathfrak{a}$ *ein beliebiges Ideal aus R, so gilt eine eindeutige Produktzerlegung* $\mathfrak{a} = \mathfrak{q}_1 \cdot \mathfrak{q}_2 \cdot \ldots \cdot \mathfrak{q}_\sigma$, *wobei die* $\mathfrak{q}_i$ *gegenseitig teilerfremde Primärideale bedeuten*[6]).

Zu jedem Ideal $\mathfrak{a}$ *gibt es einen endlichen Exponenten* $\varrho_{\mathfrak{a}}$, *so daß* $\mathfrak{a}^{\varrho_{\mathfrak{a}}} = \mathfrak{a}^{\varrho_{\mathfrak{a}}+1}$ *wird, insbesondere existiert zu einem beliebigen speziellen zer-*

[4]) Hilfssatz 1 ist im wesentlichen mit Satz 2, F. § 2 identisch.

[5]) A. II § 2, vgl. ferner die Entwicklungen bei F. § 4, wo der Zerlegungssatz ohne idealtheoretische Hilfsmittel bewiesen ist.

[6]) A. II. § 2.

legbaren Ring eine natürliche Zahl ϱ, *so daß für* $\mathfrak{a} \neq 0$ *immer* $\mathfrak{a}^{\varrho} = (0)$ *ist, oder, was dasselbe bedeutet, ein Produkt von* ϱ *Nullteilern stets verschwindet*[7]).

Aus der Tatsache, daß jedes Ideal aus R ein Hauptideal ist, ergibt sich ferner die wichtige Folgerung: *Es gibt in* R *keine ins Unendliche laufende Kette von Idealen* $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_i, \ldots$, *bei der allgemein das Ideal* $\mathfrak{a}_i$ *ein echter Teiler von* $\mathfrak{a}_{i-1}$ *ist*[8]).

Denn der größte gemeinschaftliche Teiler der Ideale $\mathfrak{a}_i$ ist selbst ein Ideal $\mathfrak{d} = (d)$ und unter unsern Vor. muß das Element d für ein endliches ν im Ideale $\mathfrak{a}_\nu$ auftreten. Dann aber wird $\mathfrak{a}_\nu = (d)$, und die Kette bricht mit $\mathfrak{a}_\nu$ ab.

Aus dem zuletzt gewonnenen Ergebnis und aus Hilfssatz 1 folgt leicht:
sind.

Satz 1. *Für jedes Ideal* $\mathfrak{a}$ *aus* R *gilt eine Gleichung*

$$\mathfrak{a} = \mathfrak{p}_1^{\varrho_1} \cdot \mathfrak{p}_2^{\varrho_2} \cdot \ldots \cdot \mathfrak{p}_\sigma^{\varrho_\sigma},$$

wobei die $\mathfrak{p}_i$ *teilerfremde Primideale bedeuten.*

Da in einem zerlegbaren Ring zwei verschiedene Primideale stets teilerfremd sind, so brauchen wir nur zu zeigen, daß sich jedes Ideal $\mathfrak{a}$ als Produkt von Primidealen darstellen läßt, dann ergibt sich durch Zusammenfassung gleicher Faktoren die Behauptung.

Sollte nun $\mathfrak{a}$ nicht als Produkt endlich vieler Primideale darstellbar sein, so müßte nach Hilfssatz 1 sicher eine Gleichung $\mathfrak{a} = \mathfrak{a}_1 \cdot \mathfrak{a}_2$ bestehen, wobei $\mathfrak{a}_1$ und $\mathfrak{a}_2$ echte Teiler von $\mathfrak{a}$ wären (denn jedes Ideal ohne von $\mathfrak{o}$ verschiedenen echten Teiler ist ja evidenterweise selbst Primideal). $\mathfrak{a}_1$ und $\mathfrak{a}_2$ können nun nicht beide als Produkt endlich vieler Primideale darstellbar sein, denn sonst gälte ja wegen $\mathfrak{a} = \mathfrak{a}_1 \cdot \mathfrak{a}_2$ das gleiche von $\mathfrak{a}$. Ist nun $\mathfrak{a}_1$ nicht als Produkt endlich vieler Primideale darstellbar, so haben wir eine Gleichung $\mathfrak{a}_1 = \mathfrak{a}_{11} \cdot \mathfrak{a}_{12}$, wobei, wie aus den vorhin bei $\mathfrak{a}$ angewandten Schlüssen folgt, bei geeigneter Bezeichnung $\mathfrak{a}_{11}$ einen nicht als Produkt von endlich viel Primidealen darstellbaren echten Teiler von $\mathfrak{a}_1$ bedeutet. Indem man jetzt auf $\mathfrak{a}_{11}$ dieselbe Schlußweise anwendet, wie früher auf $\mathfrak{a}$ und $\mathfrak{a}_1$ usw., erkennt man, daß jedes Ideal $\mathfrak{a}$ aus R als Produkt endlich vieler Primideale darstellbar sein muß, weil es andernfalls in R eine ins Unendliche laufende echte Teilerkette $\mathfrak{a}, \mathfrak{a}_1, \mathfrak{a}_{11}, \ldots$ gäbe.

Da in einem zerlegbaren Ring nach den in A. II gewonnenen allgemeinen Resultaten[9]) ein Ideal $\mathfrak{q}$ dann und nur dann Primärideal ist, wenn

---

[7]) A. II. § 2.

[8]) Vgl. N. § 1 S. 30, wo der entsprechende Satz unter der allgemeineren Vor. bewiesen ist, daß jedes Ideal aus R eine endliche Basis besitzt.

[9]) Vgl. A. II.

es durch ein einziges (von $\mathfrak{o}$ verschiedenes) Primideal teilbar ist, so können wir aus Satz 1 unmittelbar folgern:

Satz 2. *Die Potenzen der Primideale, und nur diese, sind in R Primärideale*[10]).

Die Produktzerlegung $\mathfrak{a} = \mathfrak{p}_1^{\varrho_1} \cdot \mathfrak{p}_2^{\varrho_2} \cdot \ldots \cdot \mathfrak{p}_\sigma^{\varrho_\sigma}$ *ist also mit der Produktzerlegung* $\mathfrak{a} = \mathfrak{q}_1 \cdot \mathfrak{q}_2 \cdot \ldots \cdot \mathfrak{q}_\sigma$, *die wir oben auf Grund der allgemeinen Ergebnisse von* A. II *eingeführt haben, identisch, d. h. es ist bei geeigneter Numerierung* $\mathfrak{p}_i^{\varrho_i} = \mathfrak{q}_i$ $(i = 1, 2, \ldots, \sigma)$. *Dabei sind die Exponenten* ϱ_i, *eindeutig bestimmt, falls man sie stets so klein wählt, daß* $\mathfrak{p}_i^{\varrho_i - 1} \neq \mathfrak{p}_i^{\varrho_i}$ *wird.*

Aus Satz 1 *und* 2 *geht hervor, daß die durch Axiom* I *und* II *charakterisierten zerlegbaren Ringe mit den von Herrn Fraenkel behandelten „zerlegbaren Ringen mit endlich viel wesentlich verschiedenen Nullteilern“ identisch sind.*

Sind a_1 und a_2 zwei Basiselemente desselben Ideals — wir wollen a_1 und a_2 in diesem Fall äquivalent nennen —, so unterscheiden sich a_1 und a_2 nach den allgemeinen Ergebnissen von A. II bzw. F. nur um einen Einheitsfaktor. Bezeichnen wir jedes Basiselement eines Primideals als „Primteiler“ (der Null), so können wir daher sagen: *Die zerlegbaren Ringe sind diejenigen Ringbereiche, in denen es nur Nullteiler und Einheiten gibt, und in denen sich jedes Element bis auf Einheitsfaktoren eindeutig als Produkt von Primteilern darstellen läßt.* Von dieser Definition der zerlegbaren Ringe kann man ausgehen, falls man die Idealtheorie vermeiden will.

Die speziellen Ringe, auf die man einen allgemeinen zerlegbaren Ring zurückführen kann, sind, wie aus den Ergebnissen des zweiten Teils bzw. der Fraenkelschen Arbeit folgt, und wie man übrigens auch leicht mit Hilfe der Sätze 1 und 2 zeigen kann, ebenfalls zerlegbar, und *zwar bestehen die sämtlichen vom Einheitsideal verschiedenen Ideale eines speziellen zerlegbaren Rings aus dem Nullteilerprimideal* $\mathfrak{p}^* = (p)$ *und dessen Potenzen* $\mathfrak{p}^{*2} = (p^2), \ldots, \mathfrak{p}^{*\varrho} = (p^\varrho) = (0)$.[11]) Es ist somit bei den speziellen zerlegbaren Ringen eine noch viel weitergehende Analogie mit dem Restklassensystem nach einer Primzahlpotenz vorhanden, als wie wir sie bei dem im ersten Teil behandelten umfassenderen Fall fanden.

[10]) Man beachte, daß gleichzeitig mit $\mathfrak{p}$ auch jede Potenz von $\mathfrak{p}$ zu allen von $\mathfrak{p}$ verschiedenen Primidealen teilerfremd ist!

[11]) Vgl. den Hilfssatz von A. II § 2, sowie F. § 4 Satz 7. (Nach der bei F. gegebenen Definition sind ja die bei F. als „einfach“, hier als „speziell“ bezeichneten zerlegbaren Ringe im wesentlichen durch die eben formulierte Eigenschaft der Ideale charakterisiert.)

Die wichtigsten Beispiele für zerlegbare Ringe sind neben den Restklassensystemen nach einer natürlichen Zahl die Restklassensysteme nach einem Ideal eines algebraischen Zahlkörpers. Wir werden auf das letztere Beispiel in § 4 bei Behandlung der endlichen zerlegbaren Ringe zurückkommen.

§ 2.

Polynomideale in speziellen zerlegbaren Ringen.

Es sei R ein beliebiger spezieller zerlegbarer Ring. Mit $\mathfrak{p}^*$ bezeichnen wir gemäß der bereits in § 1 benutzten Terminologie sein Nullteilerprimideal, unter p wollen wir stets einen Primteiler, also ein Basiselement von $\mathfrak{p}^*$, verstehen. *Da nach einer in § 1 gemachten Bemerkung die Ideale* $\mathfrak{o}, \mathfrak{p}^*, \mathfrak{p}^{*2}, \ldots, \mathfrak{p}^{*\varrho} = (0)$ *die einzigen in R vorkommenden Ideale sind, so läßt sich jedes Element aus R in der Form $a = r \cdot p^\sigma$ darstellen, wobei r eine Einheit bedeutet. Dabei ist der Exponent σ für $a \neq 0$ eindeutig bestimmt.*

Die Theorie der algebraischen und transzendenten Erweiterungen eines speziellen zerlegbaren Ringes läßt sich nun z. T. wesentlich einfacher gestalten, z. T. beträchtlich weiter ausbauen, als es im allgemeinen möglich gewesen war, und zwar ist einer der Gründe der, daß, wie in diesem Paragraphen gezeigt werden soll, in unserm Sonderfall ein tieferer Einblick in die Natur des zu R gehörigen Polynomrings R_f möglich ist.

Es sollen zunächst die Ideale aus R_f untersucht werden. Unter $\mathfrak{p}_f^*$ wollen wir in üblicher Weise das aus allen Nullteilern bestehende Primideal verstehen. Die Ideale $\mathfrak{p}_f^{*i}$ $(i = 1, 2, \ldots, \varrho)$ sind dann (ebenso wie die Ideale $\mathfrak{p}^{*i}$ aus R) Hauptideale, denn es ist $\mathfrak{p}_f^{*i} = (p^i)$. Es sei jetzt $\mathfrak{a}$ ein beliebiges reguläres oder nicht reguläres Ideal aus R_f. Wir betrachten die Reihe der Ideale $\mathfrak{a} = \mathfrak{a}_0 = \mathfrak{a} : \mathfrak{p}^{*0}$; $\mathfrak{a}_1 = \mathfrak{a} : \mathfrak{p}^*$; $\mathfrak{a}_2 = \mathfrak{a} : \mathfrak{p}^{*2}$ usw. Nach der Definition des Idealquotienten[12]) ist $\mathfrak{a}_i$ der größte gemeinschaftliche Teiler aller derjenigen Ideale $\mathfrak{b}$, für die die Kongruenz $\mathfrak{b} \cdot \mathfrak{p}^{*i} \equiv 0\,(\mathfrak{a})$ gilt, und es stellt daher $\mathfrak{a}_{i+1}$ einen (echten oder unechten) Teiler von $\mathfrak{a}_i$ dar. Wegen $\mathfrak{a} : \mathfrak{p}^{*\varrho} = \mathfrak{a} : (0) = (r_\varepsilon)$ kommt in der Reihe $\mathfrak{a}_0, \mathfrak{a}_1, \ldots, \mathfrak{a}_\varrho$ sicher ein reguläres Ideal vor.

Satz 3. *Ist λ die kleinste natürliche Zahl, für die $\mathfrak{a}_\lambda$ regulär ist, so gilt die Gleichung* $\mathfrak{a} = \mathfrak{a}_\lambda \cdot \mathfrak{p}^{*\lambda}$.

Es ist wegen $\mathfrak{a}_\lambda \cdot \mathfrak{p}^{*\lambda} \equiv 0\,(\mathfrak{a})$ nur nachzuweisen, daß auch umgekehrt die Kongruenz $\mathfrak{a} \equiv 0\,(\mathfrak{a}_\lambda \cdot \mathfrak{p}^{*\lambda})$ gilt. Das ist aber unter unsern Voraussetzungen über λ trivial, denn es muß jedes Element aus $\mathfrak{a}$ die Gestalt

---

[12]) Vgl. A. I § 1.

$a(x) = p^\lambda \cdot a'(x)$ besitzen, wobei p^λ durch $\mathfrak{p}^{*\lambda}$ und $a'(x)$ durch $\mathfrak{a}_\lambda$ teilbar ist. Satz 3 zeigt, daß sich in R_f die Theorie der nicht regulären Ideale auf die der regulären zurückführen läßt. Wir beschäftigen uns daher in Zukunft im wesentlichen mit den regulären Idealen.

Satz 4. *Jedes reguläre*[13]) *Ideal aus R_f besitzt eine endliche Basis, und zwar von höchstens ϱ Elementen.*

Bedeutet nämlich $f_i(x)$ eine reguläre Funktion niedrigsten Grades aus $\mathfrak{a}_i$ $(i = 0, 1, \ldots, \varrho - 1)$, so gilt die Gleichung

$$(f_0(x), p \cdot f_1(x), \ldots, p^{\varrho-1} \cdot f_{\varrho-1}(x)) = \mathfrak{a}.$$

In der Tat, ist $a(x)$ ein beliebiges Element aus $\mathfrak{a}$, so haben wir

$$a(x) = b_0(x) \cdot f_0(x) + p \cdot a_1(x); \qquad a_1(x) \equiv 0(\mathfrak{a}_1),$$

also

$$a(x) = b_0(x) \cdot f_0(x) + p \cdot b_1(x) \cdot f_1(x) + p^2 \cdot a_2(x); \quad a_2(x) \equiv 0(\mathfrak{a}_2); \quad \ldots;$$

$$a(x) = b_0(x) \cdot f_0(x) + \ldots + p^{\varrho-1} \cdot b_{\varrho-1}(x) \cdot f_{\varrho-1}(x) + 0 \cdot a_\varrho(x)$$

$$= \sum_{i=0}^{\varrho-1} b_i(x) \cdot f_i(x) \cdot p^i.$$

Eine Basis der eben angegebenen Art, bei der das $i+1$-te Glied das Produkt von p^i mit einer regulären Funktion niedrigsten Grades aus $\mathfrak{a}_i$ ist, soll als *Normalbasis von* $\mathfrak{a}$ bezeichnet werden. Besitzen nun die Funktionen niedrigsten Grades aus $\mathfrak{a}_i$ und $\mathfrak{a}_{i+1}$ den gleichen Grad, so ist jede Funktion niedrigsten Grades aus $\mathfrak{a}_i$ auch eine solche aus $\mathfrak{a}_{i+1}$, und daraus folgt unmittelbar, daß unter diesen Umständen das $i+2$-te Glied in einer Normalbasis von $\mathfrak{a}$ einfach weggelassen werden kann. Auf Grund dieser Tatsache können wir zu jedem Ideal $\mathfrak{a}$ eine „*gekürzte Normalbasis*“

$$\mathfrak{a} = (f_0(x), p^{\mu_1} \cdot f_1(x), p^{\mu_1+\mu_2} \cdot f_2(x), \ldots, p^{\mu_1+\mu_2+\cdots+\mu_\sigma} \cdot f_\sigma(x))$$

konstruieren, bei der $f_i(x)$ eine Funktion niedrigsten Grades aus $\mathfrak{a}_{\mu_1+\mu_2+\cdots+\mu_i}$ bedeutet, und bei der insbesondere der Grad von $f_i(x)$ stets niedriger ist, als der von $f_{i-1}(x)$ $(i = 1, 2, \ldots, \sigma)$. Wir bemerken noch:

Ist $g(x)$ Primfunktion, und ist $\mathfrak{a}$ ein zum Primideal

$$\mathfrak{p} = ((g(x)), \mathfrak{p}_f^*) = (g(x), p) \;{}^{14})$$

gehöriges Primärideal, bedeutet ferner $(f_0(x), p \cdot f_1(x), p^2 \cdot f_2(x), \ldots)$ eine Normalbasis von $\mathfrak{a}$, so sind die Funktionen $f_i(x)$ sämtlich zu $\mathfrak{p}$ gehörige Primärfunktionen oder Einheiten.

---

[13]) Also wegen Satz 3 und wegen der Gleichung $\mathfrak{p}^{*\lambda} = (p^\lambda)$ auch jedes nichtreguläre.

[14]) Vgl. A. I § 6 Satz 11.

In der Tat, zunächst ist nach A. I § 6 Satz 12 jedenfalls $f_0(x)$ eine zu $\mathfrak{p}$ gehörige Primärfunktion. Es sei nun (für $i \geqq 1$) $f_i(x) = h_i(x) \cdot \bar{h}_i(x)$, wobei $h_i(x)$ eine zu $\mathfrak{p}$ gehörige Primärfunktion oder eine Einheit bedeutet, während $\bar{h}_i(x)$ zu $\mathfrak{p}$ teilerfremd ist. Dann ist neben $p^i \cdot h_i(x) \cdot \bar{h}_i(x)$ auch $p^i \cdot f_0(x)$ durch $\mathfrak{a}$ teilbar, und daraus ergeben sich wegen der Teilerfremdheit von $f_0(x)$ und $\bar{h}_i(x)$ die Kongruenzen $p^i \cdot h_i(x) \equiv 0\,(\mathfrak{a})$, $h_i(x) \equiv 0\,(\mathfrak{a}_i)$. Da nun $f_i(x)$ eine Funktion niedrigsten Grades aus $\mathfrak{a}_i$ bedeutet, so muß $\bar{h}_i(x)$ eine Einheit sein, d. h. $f_i(x)$ ist, wie behauptet, primär, und gehört zu $\mathfrak{p}$, oder es ist selbst Einheit. Wir können in Anbetracht von A. I § 6 Satz 12 das gewonnene Resultat auch so formulieren:

Ist $\mathfrak{a}$ primär, so sind auch die Ideale $\mathfrak{a}_i = \mathfrak{a} : \mathfrak{p}^{*i}$, soweit sie vom Einheitsideal verschieden sind, sämtlich primär und gehören zum selben Primideal wie $\mathfrak{a}$.[15])

Für das Folgende wollen wir noch eine kurze Bemerkung machen.

Es sei $\mathfrak{a}$ ein zum Primideal $\mathfrak{p} = (g(x), p)$ gehöriges Primärideal, $(g(x)^\mu + q(x),\ p \cdot f_1(x) \ldots)$ sei eine Normalbasis von $\mathfrak{a}$, und es sei $\mu > 1$, es möge also $\mathfrak{a}$ keine Primfunktion enthalten. Wir fragen uns, wann dann $\mathfrak{a}$ durch $\mathfrak{p}^2$ teilbar ist.

Soll $\mathfrak{a}$ durch $\mathfrak{p}^2$ teilbar sein, so darf $f_1(x)$ keine Einheit sein, es muß also die Kongruenz $f_1(x) \equiv 0\,(\mathfrak{p})$ bestehen. Ist diese Bedingung erfüllt, so sind $p \cdot f_1(x)$, $p^2 \cdot f_2(x), \ldots$ sämtlich durch $\mathfrak{p}^2$ teilbar, es dreht sich also nur noch um die Frage, wann $g(x)^\mu + q(x)$ in $\mathfrak{p}^2$ enthalten ist. Soll die Kongruenz $g(x)^\mu + q(x) \equiv 0\,(\mathfrak{p}^2)$ bestehen, so muß um so mehr $g(x)^\mu + q(x) \equiv 0\,\big((g(x), p^2)\big)$ sein. Aus der letzteren Kongruenz folgt, daß $q(x)$ die Gestalt $q(x) = p \cdot g(x) \cdot h(x) + p^2 \cdot h_1(x)$ besitzen, also durch $\mathfrak{p}^2 = (g(x)^2, p \cdot g(x), p^2)$ teilbar sein muß. Wegen $\mu > 1$ ist dann auch $g(x)^\mu$ durch $\mathfrak{p}^2$ teilbar, es folgt also für $\mu > 1$ aus der Kongruenz $g(x)^\mu + q(x) \equiv 0\,\big((g(x), p^2)\big)$ rückwärts die Kongruenz $g(x)^\mu + q(x) \equiv 0\,(\mathfrak{p}^2)$ und daraus weiter $\mathfrak{a} \equiv 0\,(\mathfrak{p}^2)$.

Das gewonnene Resultat formulieren wir mit Rücksicht auf das Folgende etwas spezieller als nötig so:

Es sei $\mathfrak{a}$ ein zum regulären Primideal $\mathfrak{p}$ gehöriges Primärideal, das weder eine Primfunktion noch ein Element aus R, also insbesondere keinen Primteiler aus R enthält, $f(x)$ sei ein reguläres Polynom niedrigsten Grades aus $\mathfrak{a}$, $g(x)$ sei eine beliebige Primfunktion aus $\mathfrak{p}$. Dann ist die notwendige und hinreichende Bedingung für die Teilbarkeit von $\mathfrak{a}$ durch $\mathfrak{p}^2$ das Bestehen der Kongruenz $f(x) \equiv 0\,\big((g(x), p^2)\big)$.

---

15) Dies Ergebnis kann auch als Spezialfall aus Satz 3 der Note von W. Krull: Ein neuer Beweis für die Hauptsätze der allgemeinen Idealtheorie, Math. Annalen **90**, S. 55–65, abgeleitet werden.

§ 3.

Reguläre Erweiterungen spezieller zerlegbarer Ringe.

Wir hatten in A. II § 7 einen speziellen Erweiterungsring $\bar{R}$ des speziellen Ringes R — wo $\bar{R}$ also auch wieder nur Nullteiler und Einheiten enthält und das System aller Nullteiler ein Primideal bildet — eine *reguläre* Erweiterung von R genannt, wenn $\bar{R}$ eine reguläre Modulbasis hinsichtlich R besitzt, d. h. wenn sich aus $\bar{R}$ eine (endliche oder unendliche) Menge von Elementen $\alpha_1, \alpha_2, \ldots, \alpha_\tau, \ldots$ herausgreifen läßt, derart, daß für jedes Element α aus $\bar{R}$ eine eindeutig bestimmte Darstellung $\alpha = \sum_{i=1}^{\nu} a_i \alpha_{\tau_i}$ durch endlich viele der α_τ mit Koeffizienten a aus R gilt, wobei insbesondere bei einem Nullteiler α ausschließlich Nullteiler aus R als Koeffizienten auftreten. Im Bereich der zerlegbaren Ringe gilt nun für reguläre Erweiterungen folgender grundlegender Doppelsatz:

Satz 5. *Jede reguläre Erweiterung $\bar{R}$ eines speziellen zerlegbaren Ringes R ist selbst wieder ein spezieller zerlegbarer Ring, und zwar ist jeder Primteiler aus R auch in $\bar{R}$ Primteiler. Ist umgekehrt $\bar{R}$ ein spezieller zerlegbarer Erweiterungsring des speziellen zerlegbaren Ringes R und ist ein Primteiler aus R auch Primteiler in $\bar{R}$, so ist $\bar{R}$ eine reguläre Erweiterung von R.*

Der erste Teil unserer Behauptung folgt aus der Definition der regulären Modulbasis einfach so: Es sei $\alpha = \sum_{i=1}^{\nu} a_i \alpha_{\tau_i}$ ein beliebiges Element aus $\bar{R}$, p sei ein beliebiger Primteiler aus R. Dann stellt jedes Element a_i das Produkt einer Potenz von p mit einer Einheit aus R dar, und wir können daher σ so bestimmen, daß ν Gleichungen $a_i = p^\sigma \cdot b_i$ $(i = 1, 2, \ldots, \nu)$ bestehen, wobei die b_i Elemente aus R und nicht sämtlich Nullteiler sind. Dann aber haben wir: $\alpha = p^\sigma \cdot \sum_{i=1}^{\nu} b_i \alpha_{\tau_i}$ und das Element $\sum_{i=1}^{\nu} b_i \alpha_{\tau_i}$ muß gemäß der Definition der regulären Erweiterung eine Einheit aus $\bar{R}$ sein. Es stellt also jedes Element aus $\bar{R}$ das Produkt einer Potenz von p mit einer Einheit dar, d. h. $\bar{R}$ ist ein spezieller zerlegbarer Ring mit dem Primteiler p.

Nehmen wir nun umgekehrt von vornherein an, daß $\bar{R}$ ein spezieller zerlegbarer Ring und p gleichzeitig in R und $\bar{R}$ Primteiler ist, so können wir zunächst folgendes bemerken: Sind die Elemente $\alpha_1, \alpha_2, \ldots, \alpha_\tau, \ldots$ aus $\bar{R}$ linear unabhängig, d. h. besteht zwischen endlich vielen von ihnen keine Relation $\sum_{i=1}^{\nu} a_i \alpha_{\tau_i} = 0$ mit nicht sämtlich verschwindenden Koeffizienten aus R, so ist ein Element von der Form $\sum_{i=1}^{\nu} a_i \alpha_{\tau_i}$ nur dann Nullteiler, wenn sämtliche a_i Nullteiler sind.

In der Tat, soll $\sum_{i=1}^{\nu} a_i \alpha_{\tau_i}$ ein Nullteiler sein, so haben wir unter unsern Vor. $\sum_{i=1}^{\nu} a_i \alpha_{\tau_i} = p^{\sigma} \cdot \beta$; $\sigma > 0$. Daraus folgt aber durch Multiplikation mit $p^{\varrho-\sigma} \neq 0$:[16] $\sum_{i=1}^{\nu} (p^{\varrho-\sigma} \cdot a_i) \cdot \alpha_{\tau_i} = p^{\varrho} \cdot \beta = 0$. Wegen der linearen Unabhängigkeit der α_i folgt dann weiter $p^{\varrho-\sigma} \cdot a_i = 0$ $(i = 1, 2, \ldots, \nu)$, d. h. es müssen alle a_i durch p^{σ} teilbar, also gemäß unserer Behauptung Nullteiler sein.

Sind nun die Elemente $\alpha_1, \alpha_2, \ldots, \alpha_\tau, \ldots$ hinsichtlich R linear unabhängig, und ist α ein beliebiges Element aus $\overline{R}$, so ist entweder α von den α_τ linear unabhängig, oder es besteht eine Kongruenz $\alpha \equiv \sum_{i=1}^{\nu} a_i \alpha_{\tau_i} ((p))$. Soll nämlich die Gesamtheit der Elemente $\alpha_1, \alpha_2, \ldots, \alpha_\tau, \ldots, \alpha$ nicht linear unabhängig sein, so muß wegen der linearen Unabhängigkeit von $\alpha_1, \alpha_2, \ldots, \alpha_\tau, \ldots$ eine Gleichung $\sum_{i=1}^{\nu} a_i \alpha_{\tau_i} + a \cdot \alpha = 0$ mit von 0 verschiedenem a bestehen. Ist nun p^{σ} $(\sigma < \varrho)$ die höchste in $a_1, a_2, \ldots, a_\nu, a$ aufgehende Potenz von p, und setzen wir $a_i = p^{\sigma} \cdot b_i$, $a = p^{\sigma} \cdot b$, so folgt aus unserer Gleichung die Kongruenz $\sum_{i=1}^{\nu} b_i \cdot \alpha_{\tau_i} + b \cdot \alpha \equiv 0 (p^{\varrho-\sigma})$.[17] Wäre nun b ein Nullteiler, so müßte mindestens ein b_i eine Einheit sein, und es wäre wegen $\varrho - \sigma > 0$ das Element $\sum_{i=1}^{} b_i \alpha_{\tau_i}$ durch p teilbar und folglich ein Nullteiler, was nach dem oben Festgestellten mit der linearen Unabhängigkeit von $\alpha_1, \alpha_2, \ldots, \alpha_\tau, \ldots$ im Widerspruch stände. Es muß mithin b eine Einheit sein, und wir haben $\alpha \equiv -\sum_{i=1}^{\nu} (b^{-1} \cdot b_i) \cdot \alpha_{\tau_i} ((p))$.

Mit Hilfe der beiden eben gemachten Bemerkungen sind wir nunmehr imstande, eine reguläre Modulbasis von $\overline{R}$ hinsichtlich R zu konstruieren. Es seien $\alpha_1, \alpha_2, \ldots, \alpha_\tau, \ldots$ sämtliche Elemente von $\overline{R}$ in einer beliebigen Wohlordnung[18]). Nur wollen wir der Einfachheit halber α_1 als Einheit voraussetzen. Wir zeigen dann durch transfinite Induktion: *Für jedes τ kann man aus den Elementen α_i ($i \leqq \tau$ bzw. $i < \tau$, falls $\tau - 1$ nicht existiert) eine Teilmenge $\mathfrak{M}_\tau = \{\alpha_{\sigma_1} = \beta_1, \alpha_{\sigma_2} = \beta_2, \ldots\}$ linear unabhängiger Elemente herausgreifen, derart, daß jedes α_i für $i \leqq \tau$ bzw. $i < \tau$ einer Kongruenz $\alpha_i \equiv \sum_{i=1}^{\nu} a_i \beta_{\kappa_i} ((p))$ genügt. Dabei kann insbesondere $\mathfrak{M}_\tau$ stets*

[16]) Unter ϱ verstehen wir immer den charakteristischen Exponenten von R, so daß $p^{\varrho-1} \neq 0$; $p^{\varrho} = 0$ ist.

[17]) Man beachte, daß hier die Vor. benutzt wird, daß p einen Primteiler aus $\overline{R}$ bedeutet!

[18]) Falls $\tau - 1$ nicht existiert, entspricht der Ordnungszahl τ kein Element α_τ!

so gewählt werden, daß $\mathfrak{M}_\tau$ *die sämtlichen Mengen* $\mathfrak{M}_{\tau_1}$ $(\tau_1 < \tau)$ *enthält.* In der Tat, für $\tau = 1$ ist $\mathfrak{M}_1 = \{\alpha_1\}$ die gewünschte Menge, gibt es ferner für $\tau - 1$ eine Menge $\mathfrak{M}_{\tau-1}$, so können wir nach dem oben Festgestellten $\mathfrak{M}_\tau = \{\mathfrak{M}_{\tau-1}, \alpha_\tau\}$ bzw. $\mathfrak{M}_\tau = \mathfrak{M}_{\tau-1}$ setzen, je nachdem α_τ von den Elementen der Menge $\mathfrak{M}_{\tau-1}$ linear unabhängig ist oder nicht; und ist schließlich die Behauptung im Falle, daß $\tau - 1$ nicht existiert, für alle $\tau_1 < \tau$ richtig, so gilt sie auch für $\tau_1 = \tau$, denn man braucht für $\mathfrak{M}_\tau$ dann nur die Vereinigungsmenge aller $\mathfrak{M}_{\tau_1}$ $(\tau_1 < \tau)$ zu wählen[19]).

Verstehen wir nun unter $\mathfrak{M} = \{\beta_1, \beta_2, \ldots, \beta_\tau, \ldots\}$ die Vereinigungsmenge aller $\mathfrak{M}_\tau$, so sind die Elemente β_τ ersichtlich alle linear unabhängig, und es kann daher, wie oben festgestellt, $\beta = \sum_{i=1}^{\nu} a_i \beta_{\tau_i}$ nur dann Nullteiler sein, wenn alle a_i Nullteiler sind. *Daraus folgt, daß die Elemente* β_τ *eine reguläre Modulbasis von* $\overline{R}$ *hinsichtlich* R *bilden, sofern wir nur zeigen können, daß sich jedes Element aus* $\overline{R}$ *linear durch die* β_τ *darstellen läßt.* Das ergibt sich aber ohne Schwierigkeit aus dem in A. II so oft benutzten „Korrektionsgliederverfahren". In der Tat, ist α ein beliebiges Element aus $\overline{R}$, so haben wir angesichts der Konstruktion der Menge $\mathfrak{M}$ eine Gleichung $\alpha = \sum_{i=1}^{\nu_1} a_i^{(1)} \beta_{\tau_i^{(1)}} + p \cdot \alpha_1$. Indem wir jetzt α_1 modulo p durch die β_τ ausdrücken, kommen wir weiter zu einer Gleichung $\alpha = \sum_{i=1}^{\nu_2} a_i^{(2)} \beta_{\tau_i^{(2)}} + p^2 \cdot \alpha_2$ und nach ϱ Schritten finden wir: $\alpha = \sum_{i=1}^{\nu_\varrho} a_i^{(\varrho)} \beta_{\tau_i^{(\varrho)}}$. Die Elemente β_τ bilden also wirklich eine reguläre Modulbasis von $\overline{R}$ hinsichtlich R, es gilt nicht nur der erste Teil von Satz 5, sondern auch die Umkehrung.

Die für Satz 5 *wesentliche Bedingung, daß* R *und* $\overline{R}$ *den gleichen Primteiler* p *besitzen, ist mit der Forderung identisch, daß der charakteristische Exponent* ϱ' *von* $\overline{R}$ *gleich dem charakteristischen Exponenten* ϱ *von* R *ist.* In der Tat, ist p' ein Primteiler aus $\overline{R}$, p ein solcher aus R, so ist $p = r \cdot p'^{\lambda}$, wobei r eine Einheit bedeutet, und wegen $p^{\varrho-1} \neq 0$; $p^\varrho = 0$ ergibt sich daraus für ϱ die Ungleichung: $(\varrho - 1) \cdot \lambda < \varrho' \leqq \varrho \cdot \lambda$. Daraus folgt, daß ϱ dann und nur dann gleich ϱ' ist, wenn die Gleichung $\lambda = 1$ gilt, d. h. wenn p auch in $\overline{R}$ Primteiler ist.

Auf Grund der gemachten Bemerkung können wir Satz 5 kurz so aussprechen:

Die regulären Erweiterungen des speziellen zerlegbaren Ringes R *sind die einzigen speziellen zerlegbaren Erweiterungsringe mit dem gleichen charakteristischen Exponenten.*

---

[19]) Vgl. zu diesem Beweis den ganz analogen Beweis von Satz 21, A. II § 8!

Aus dem gewonnenen Ergebnis folgt insbesondere:

Ist R ein spezieller zerlegbarer Ring mit dem Primteiler p, so ist jede regulär algebraische und transzendente Erweiterung $\overline{R}$ ein spezieller zerlegbarer Ring mit dem gleichen Primteiler.

Denn die regulär algebraischen und transzendenten Erweiterungen besitzen ja, wie in A. II § 7 gezeigt wurde, stets eine reguläre Modulbasis hinsichtlich des Ausgangsringes.

Zum Schluß dieses Paragraphen wollen wir noch einen Satz beweisen, aus dem hervorgeht, daß die in A. I und A. II gewonnenen Resultate bei zerlegbaren Ringen in wesentlich einfacherer Weise abgeleitet werden können, als es im umfassenden Fall möglich war. Wir zeigen nämlich:

Satz 6. *Ist α ein Element aus einer beliebigen, speziellen Erweiterung des speziellen zerlegbaren Ringes R, so ist α hinsichtlich R regulär algebraisch, wenn es Nullstelle einer Primfunktion aus R_f ist, es ist hinsichtlich R regulär transzendent, wenn es Nullstelle keiner regulären Funktion aus R_f ist.*

Um den ersten Teil unseres Satzes zu beweisen, müssen wir zeigen, daß α als Nullstelle von $g(x)$ keiner Gleichung von niedrigerem Grade als $g(x)$ mit Koeffizienten aus R genügen kann. In der Tat, ist $a(x)=0$ eine solche Gleichung, so können wir $a(x)$ auf die Gestalt $a(x)=p^{\mu}\cdot f(x)$ bringen, wobei $f(x)$ eine reguläre Funktion von niedrigerem Grade als $g(x)$ bedeutet. Dann aber müssen $f(x)$ und $g(x)$ teilerfremd sein, und aus $g(\alpha)=0$, $a(\alpha)=0$ folgt $p^{\mu}=0$, d. h. $a(x)$ muß identisch verschwinden. — In ähnlicher Weise zeigen wir zum Beweise des zweiten Teiles unseres Satzes, daß α notwendig Nullstelle eines regulären Polynoms sein muß, falls es überhaupt einer nicht identisch bestehenden Gleichung mit Koeffizienten aus R genügt. Ist nämlich $a(\alpha)=0$, so setzen wir wie oben $a(x)=p^{\mu}\cdot f(x)$, wobei $f(x)$ ein reguläres Polynom bedeutet. Sollte nun $p^{\mu}\neq 0$ sein, so ist $f(\alpha)$ ein Nullteiler des Erweiterungsringes, dem α angehört. Da aber dieser Erweiterungsring nach Vor. speziell ist, so haben wir für eine gewisse natürliche Zahl ϱ': $f^{\varrho'}(\alpha)=0$, d. h. α ist Nullstelle des regulären Polynoms $f^{\varrho'}(x)$.

Satz 6 konnte im umfassenden Fall nur unter der einschränkenden Vor. bewiesen werden, daß α einer *regulären* Erweiterung von R angehört. Man könnte nun vielleicht auf Grund des hier gewonnenen weitergehenden Resultats annehmen, daß sich etwa die Theorie der unvollkommenen zerlegbaren Ringe wesentlich gründlicher ausbauen ließe, als es im umfassenden Fall möglich war. Daß dem nicht so ist, lehren die Gegenbeispiele, durch die wir in A. I und A. II zeigten, daß man bei unvollkommenen Ringen nicht zu den gleichen Isomorphiekriterien gelangen kann wie bei den vollkommenen; denn diese Gegenbeispiele sind dem Gebiet der zerlegbaren Ringe entnommen.

§ 4.

Allgemeine einfache algebraische Erweiterungen zerlegbarer Ringe.

Wir stellen uns in diesem Paragraphen die Aufgabe, den allgemeinsten Fall zu untersuchen, in dem wir von dem speziellen zerlegbaren Ringe R durch Adjunktion eines einzigen Elementes α wiederum zu einem speziellen zerlegbaren Ringe $R(\alpha)$ gelangen. Ohne Interesse ist die Möglichkeit, daß α Nullstelle von überhaupt keiner Funktion aus R_f ist. Denn dann gelangen wir offenbar zu einer regulär transzendenten Erweiterung von R, wenn wir die Gesamtheit aller rationalen Funktionen in α mit Koeffizienten aus R bilden, bei denen das Nennerpolynom mindestens einen regulären Koeffizienten besitzt.

Wir beschäftigen uns daher in Zukunft nur mit den Fällen, in denen α Nullstelle mindestens eines Polynoms aus R_f ist — es soll $R(\alpha)$ dann als *allgemeine algebraische Erweiterung* von R bezeichnet werden. *Die Gesamtheit der Polynome in x, die für $x = \alpha$ verschwinden, bilden ein Ideal $\mathfrak{a}$ aus R_f, und dieses Ideal muß, wie aus dem Satz 6 des vorangehenden Paragraphen folgt, mindestens eine reguläre Funktion enthalten.* Ferner ist ohne weiteres klar, daß in $\mathfrak{a}$ kein von 0 verschiedenes Element aus R vorkommen kann, denn ein Element aus R soll ja in dem Erweiterungsring $\overline{R}$ nur dann verschwinden, wenn es bereits in R verschwindet. *Schließlich erkennt man leicht, daß das Ideal $\mathfrak{a}$ primär sein muß, falls $R(\alpha)$ ein spezieller zerlegbarer Ring sein soll.*

Wäre nämlich $\mathfrak{a}$ nicht primär, so wäre es das Produkt von zwei teilerfremden Idealen $\mathfrak{a}_1$ und $\mathfrak{a}_2$. Dann aber könnte man aus $\mathfrak{a}_1$ und $\mathfrak{a}_2$ zwei Funktionen $f_1(x)$ und $f_2(x)$ auswählen, die teilerfremd, und daher sicher nicht durch $\mathfrak{a}$ teilbar wären. Es gäbe mithin wegen $f_1(x) \cdot f_2(x) \equiv 0\ (\mathfrak{a})$ und der daraus folgenden Gleichung $f_1(\alpha) \cdot f_2(\alpha) = 0$ in $R(\alpha)$ zwei teilerfremde Nullteiler, nämlich $f_1(\alpha)$ und $f_2(\alpha)$, $R(\alpha)$ wäre also sicher nicht speziell. Als primäres Ideal muß $\mathfrak{a}$ nach den Entwicklungen von § 2 eine gekürzte Normalbasis

$$\mathfrak{a} = (h(x),\ p^{\mu_1} \cdot h_1(x),\ p^{\mu_1 + \mu_2} \cdot h_2(x),\ \ldots,\ p^{\mu_1 + \mu_2 + \cdots + \mu_\sigma} \cdot h_\sigma(x))$$

besitzen, wobei p einen Primteiler aus R bedeutet, und die Funktionen $h(x) = h_0(x), h_1(x), \ldots, h_\sigma(x)$ sämtlich zum Primideal $\mathfrak{p} = (g(x), p)$ gehörige Primärfunktionen sind[20]), mithin die Gestalt $h_i(x) = l_i(x) \cdot g_i(x)$ besitzen.

Wir behandeln zunächst den Fall, daß $\overline{R} = R(\alpha)$ denselben charakteristischen Exponenten wie R hat, und daß infolgedessen ein Primteiler p aus R auch in $\overline{R}$ Primteiler ist. Aus den Entwicklungen von § 3 kann man leicht schließen, daß in diesem Falle $\overline{R}$ eine regulär algebraische Erweiterung von R darstellen muß, man kann aber diese Tatsache auch ohne die oben angestellten allgemeinen Überlegungen einfach so einsehen:

Da das Element $g(\alpha)$ offenbar in $\overline{R}$ ein Nullteiler sein muß, und da p auch in $\overline{R}$ Primteilereigenschaft besitzen soll, so muß eine Gleichung $p^\mu \cdot f(\alpha) = g(\alpha)$ bestehen, wobei $f(\alpha)$ ein reguläres Element aus $\overline{R}$ bedeutet, und diese Gleichung ist mit der Kongruenz $p^\mu \cdot f(x) \equiv g(x)$ $(\mathfrak{a})$ identisch. $\mathfrak{a}$ enthält also die Primfunktion $g(x) - p^\mu \cdot f(x)$, und muß mit dem durch diese Primfunktion erzeugten Ideale $(g(x))$ identisch sein, weil andernfalls in $\mathfrak{a}$ entgegen unserer Voraussetzung ein von 0 verschiedenes Element aus R aufträte[21]).

Der Ring $\overline{R}$ ist demnach dem Restklassensystem nach einer Primfunktion aus R_f isomorph, d. h. er ist eine einfache reguläre algebraische Erweiterung von R, und wir können den Satz aussprechen:

Satz 7. *Ist α nicht hinsichtlich R transzendent und ist $R(\alpha)$ ein spezieller zerlegbarer Ring mit den gleichen charakteristischen Exponenten wie R, so ist $R(\alpha)$ eine regulär algebraische Erweiterung des Ringes R.*

In einfacher Weise läßt sich die Frage nach der allgemeinsten algebraischen Erweiterung noch in dem Falle beantworten, daß R ein Körper ist, also den charakteristischen Exponenten $\varrho = 1$ besitzt. Hier hat jedes primäre Ideal $\mathfrak{a}$ aus R_f die Gestalt $(g(x))^{\varrho'}$, wobei $g(x)$ eine Primfunktion bedeutet, und man sieht unmittelbar, daß der durch Adjunktion einer Nullstelle α von $\mathfrak{a}$ entstehende Ring $\overline{R} = R(\alpha)$ einen zerlegbaren Ring mit dem charakteristischen Exponenten ϱ' und dem Primteiler $g(\alpha)$ darstellt.

Satz 8. *Die allgemeinste einfache algebraische Erweiterung, die von einem Körper R zu einem speziellen zerlegbaren Ring mit dem charakteristischen Exponenten ϱ' führt, entsteht aus R durch Adjunktion einer Nullstelle der ϱ'*-ten *Potenz einer Primfunktion $g(x)$ aus R_f, d. h. sie ist zu dem Restklassensystem nach $(g(x)^{\varrho'})$ isomorph.*

---

[20]) Man beachte hier, daß die Möglichkeit, daß eine der Funktionen $h_i(x)$ eine Einheit ist, durch die Voraussetzung, $\mathfrak{a}$ solle kein Element aus R enthalten, ausgeschlossen ist!

[21]) Man beachte, daß $g(x)$ als Primfunktion zu jeder regulären Funktion niedrigeren Grades teilerfremd ist.

Wir betrachten jetzt den allgemeinen Fall, daß R einen von 0 verschiedenen Primteiler p enthält, der im Ringe $\bar{R}$ die Primteilereigenschaft verliert. Es sei dann p' ein Primteiler aus $\bar{R}$. Als Nullteiler muß p' die Gestalt $p' = g(\alpha) \cdot k(\alpha) + p \cdot k_1(\alpha)$ besitzen, wobei wir $k_1(\alpha)$ von niedrigerem Grade als $g(\alpha)$ annehmen dürfen. Wäre nämlich $p' = g(\alpha) \cdot k(\alpha) + r(\alpha)$, wobei $r(\alpha)$ eine reguläre Funktion von niedrigerem Grade als $g(x)$ bedeutet, so wären $h(x) = l(x) \cdot g(x) + q(x)$ und $g(x) \cdot k(x) + r(x)$ teilerfremd.

Zwischen p und p' muß eine Gleichung von der Form $p \cdot m(\alpha) = p'^{\lambda}$ $(\lambda > 1)$ bestehen, wobei $m(\alpha)$ ein reguläres Element aus $\bar{R}$ bedeutet. Aus diesem Grunde müssen $m(x)$ und $g(x)$ teilerfremd sein und $m(x)$ besitzt daher die Form $m(x) = m_1(x) \cdot g(x) + r(x)$, wobei $r(x)$ eine reguläre Funktion bedeutet, deren Ordnung niedriger ist als der Grad von $g(x)$. Die zwischen p und p' bestehende Gleichung ist identisch mit einer Kongruenz von der Form

$$(1) \qquad p \cdot m_1(x) \cdot g(x) + p \cdot r(x) - F(x) \cdot g(x) - p^{\lambda} \cdot k_1(x)^{\lambda} \equiv 0\,(\mathfrak{a}),$$

dabei bezeichnet $F(x) \cdot g(x)$ den durch $g(x)$ teilbaren Bestandteil von $(k(x) \cdot g(x) + p \cdot k_1(x))^{\lambda}$. Ist nun $\mathfrak{a}$ durch das Ideal $(g(x), p^2)$ teilbar, so geht aus der Kongruenz (1) die Kongruenz

$$(2) \qquad p \cdot r(x) - p^{\lambda} \cdot k_1(x)^{\lambda} \equiv 0\,((g(x), p^2))$$

hervor, und daraus folgt weiter wegen $\lambda > 1$

$$(3) \qquad p \cdot r(x) \equiv 0 \;\; ((g(x), p^2)).$$

Die Kongruenz (3) ist aber unmöglich, weil $r(x)$ eine reguläre Funktion von niedrigerem Grade als $g(x)$ ist. *Als notwendige Bedingung dafür, daß $\bar{R}$ einen speziellen zerlegbaren Ring darstellt, ergibt sich also, daß das Ideal $\mathfrak{a}$ und mithin nach einer oben gemachten Bemerkung alle durch $\mathfrak{a}$ teilbaren Funktionen niedrigsten Grades nicht durch das Ideal $(g(x), p^2)$, also auch nicht durch das Ideal $(g(x), p)^2$ teilbar sein dürfen.*

Es ist nun zu untersuchen, wie weit diese Bedingung auch hinreicht. Zunächst betrachten wir den Fall, daß $\mathfrak{a} = (h(x))$ ein Hauptideal ist. Jeder Nullteiler des Ringes $\bar{R}$ besitzt dann die Gestalt $k(\alpha) \cdot g(\alpha) + p^{\sigma} \cdot r(\alpha)$, wobei $r(\alpha)$ eine reguläre Funktion von niedrigerem Grade als $g(\alpha)$ bedeutet, und umgekehrt ist jedes Element dieser Form ein Nullteiler. Der Beweis dieser Tatsache folgt mühelos daraus, daß $h(x)$ eine zum Primideal $(g(x), p)$ gehörige Primärfunktion ist. Machen wir jetzt die Annahme, daß $h(x)$ nicht durch das Ideal $(g(x), p^2)$ teilbar ist, so muß $h(x)$ die Gestalt $h(x) = l(x) \cdot g(x) + q(x)$ besitzen, wobei $q(x)$ von niedrigerem Grade als $g(x)$ und nicht durch p^2 teilbar ist, d. h. wir haben $q(x) = p \cdot r_1(x)$, wobei $r_1(x)$ eine reguläre Funktion bedeutet, die von niedrigerem Grade als $g(x)$, und mithin zu $g(x)$ und $h(x)$ teilerfremd ist. Da nun $h(x)$ als Primärfunktion die Gestalt $h(x) = e(x) \cdot g(x)^{\mu} + Q(x)$ besitzen muß, so ergibt sich aus der Gleichung $h(\alpha) = 0$ eine Gleichung von der Form $g(\alpha)^{\mu} = p \cdot e^{-1}(\alpha) \cdot (F(\alpha) \cdot g(\alpha) + r_1(\alpha))$, und es muß $F(\alpha) \cdot g(\alpha) + r_1(\alpha)$ eine Einheit aus $\overline{R}$ sein, weil, wie oben bemerkt, $h(x)$ und $r_1(x)$, also auch $h(x)$ und $F(x) \cdot g(x) + r_1(x)$ teilerfremd sind. Daher gilt in $\overline{R}$ eine Gleichung $p = g(\alpha)^{\mu} \cdot G(\alpha)$ und jeder Nullteiler aus $\overline{R}$ läßt sich als Produkt einer Einheit mit einer Potenz von $g(\alpha)$ darstellen, d. h. *$\overline{R}$ ist ein spezieller zerlegbarer Ring mit dem Primteiler* $g(\alpha)$. Es handelt sich um die Bestimmung des zu $\overline{R}$ gehörigen charakteristischen Exponenten ϱ'. Jedenfalls ist $g(\alpha)^{\mu \cdot \varrho} = 0$, d. h. es ist $\varrho' \leqq \mu \cdot \varrho$. Wäre aber $\varrho' < \mu \cdot \varrho$, so wäre wegen des Bestehens der Gleichung $p = g(\alpha)^{\mu} \cdot G(\alpha)$ auch $p^{\nu_1} \cdot g(\alpha)^{\nu_2} = 0$, wenn man

$$\varrho' = \nu_1 \cdot \mu + \nu_2 \quad (\nu_1 < \varrho,\ \nu_2 < \mu)$$

setzte. Das ist aber unmöglich, weil $g(x)^{\nu_2} \cdot p^{\nu_1}$ von niedrigerem Grade als $h(x)$ und $p^{\nu_1} \neq 0$ ist. *Wenn also $\overline{R}$ das Restklassensystem nach einer Primärfunktion darstellt, so ist sein charakteristischer Exponent durch $\mu \cdot \varrho$ gegeben.*

Wir wenden uns jetzt zur Behandlung des allgemeinsten Falles. Die bisher angestellten Überlegungen, durch die wir zeigten, daß $\overline{R}$ ein spezieller zerlegbarer Ring ist, falls $\mathfrak{a}$ nicht durch $(g(x), p)^2$ teilbar ist, lassen sich unmittelbar hierauf übertragen. Wir haben noch zu untersuchen, welchen Beschränkungen das Ideal $\mathfrak{a}$ dadurch unterworfen ist, daß wir fordern, es solle keine Elemente aus R enthalten. Zu diesem Zwecke betrachten wir eine gekürzte Normalbasis von $\mathfrak{a}$:

$$\mathfrak{a} = (h(x),\ p^{\mu_1} \cdot h_1(x),\ p^{\mu_1 + \mu_2} \cdot h_2(x) \ldots). \tag{4}$$

Dabei dürfen wir annehmen, daß in (4) allgemein $\mu_i > 0$ ist, und daß die $h_i(x)$ zur Primfunktion $g(x)$ gehörige Primärfunktionen von niedrigerem Grade als $h(x)$ bedeuten. Ist $h_1(x) = g(x)^{\nu} + q_1(x)$ $(\mu > \nu)$, so besteht infolge der speziellen Gestalt von $h(x)$ eine Kongruenz von der Form

$$h_1(x) \equiv g(x)^{\mu} \cdot k_1(x) + g(x)^{\nu} \quad ((h(x))). \tag{5}$$

(Man beachte, daß nach den für den Fall $\mathfrak{a} = (h(x))$ angestellten Überlegungen eine Kongruenz $p \equiv g(x)^{\mu} \cdot G(x)$ $((h(x)))$ gelten muß.)

Da nun die Funktionen $h(x)$ und $g(x)^{\mu - \nu} \cdot k_1(x) + r_\varepsilon$ teilerfremd sind, so gibt es eine reguläre Funktion $k_2(x)$, die der Kongruenz $k_2(x) \cdot h_1(x) \equiv g(x)^{\nu}$ $((h(x)))$ Genüge leistet. Man kann also in der

Basis von $\mathfrak{a}$ die Funktion $p^{\mu_1}\cdot h_1(x)$ durch $p^{\mu_1}\cdot g(x)^{\nu}$ ersetzen. Ferner muß $\mu_1 \geqq \varrho - 1$ sein; denn aus der Gleichung $p^{\mu_1}\cdot g(\alpha)^{\nu} = 0$ folgt $p^{\mu_1}\cdot g(\alpha)^{\mu} = 0$ und wegen des Bestehens der Gleichung $h(\alpha) = 0$ ergibt sich hieraus wegen der Gleichheit der Ideale (p) und $(g(\alpha)^{\mu})$ die Gleichung $p^{\mu_1+1} = 0$. Es ist also gemäß unserer Behauptung entweder $\mu_1 = \varrho$, und dann ist $\mathfrak{a}$ ein Hauptideal, oder es ist $\mu_1 = \varrho - 1$, und $\mathfrak{a}$ besitzt die Basis $(h(x), p^{\varrho-1}\cdot g(x)^{\nu})$ $(0 < \nu < \mu)$. Im letzteren Falle ist der charakteristische Exponent von $\overline{R}$ durch $\varrho' = \mu\cdot(\varrho - 1) + \nu$ gegeben. Das Gesamtresultat unserer Untersuchung über nicht reguläre algebraische Erweiterungen spezieller zerlegbarer Ringe fassen wir unter Beachtung der Bemerkung vom Schlusse von § 2 in dem folgenden Satze zusammen:

Satz 9. *Die allgemeinste einfache algebraische Erweiterung, die von dem speziellen zerlegbaren Ring R mit dem charakteristischen Exponenten $\varrho \geqq 2$ zu einem gleichfalls zerlegbaren speziellen Ringe $\overline{R}$ führt und die Eigenschaft besitzt, daß alle in R verschiedenen Elemente auch in $\overline{R}$ verschieden sind, besteht aus den Restklassen aller Polynome einer Variablen α mit Koeffizienten aus R nach einem nicht durch das Quadrat seines Primideals teilbaren Primärideal $\mathfrak{a}$ von der Form $(g(x)^{\mu} + q(x),\ p^{\varrho-1} g(x)^{\nu})$, wobei $g(x)$ eine Primfunktion aus dem zu $\mathfrak{a}$ gehörigen Primideal bedeutet, und die Ungleichung $0 < \nu \leqq \mu$ besteht. Die niedrigste Potenz, für die der Primteiler $p' = g(\alpha)$ aus $\overline{R}$ verschwindet, ist $\varrho' = \mu(\varrho - 1) + \nu$.*[22])

Eine spezielle Folgerung aus dem eben formulierten Theorem ist nachstehender Satz, der in einem Spezialfalle bereits von Herrn Fraenkel bewiesen wurde[23]).

Satz 10. *Ist R ein spezieller zerlegbarer Ring mit dem Exponenten $\varrho = 2$, so ist jedes Restklassensystem nach einer irreduziblen Funktion aus R_f gleichfalls ein spezieller zerlegbarer Ring.*

In der Tat, auf jeden Fall muß eine irreduzible Funktion Primärfunktion sein. Unter unseren Voraussetzungen ist aber ferner diese Primärfunktion entweder eine Primfunktion, oder sie genügt der in Satz 8 geforderten Bedingung, weil man sonst von ihr eine Primfunktion als Faktor abspalten könnte. Wir bemerken noch:

Das Restklassensystem nach einer reduziblen Primärfunktion ist nie ein spezieller zerlegbarer Ring, wenn der Ausgangsring kein Körper ist.

Ist nämlich $h(x) = (g(x)^{\nu_1} + q_1(x))\cdot(g(x)^{\nu_2} + q_2(x))$, so sind beide Faktoren durch $(g(x), p)$ und folglich $h(x)$ durch $(g(x), p)^2$ teilbar.

---

[22]) Besitzt das Ideal $\mathfrak{a}$ eine eingliedrige Basis, so ist $\nu = \mu$ zu setzen!

[23]) Über gewisse Teilbereiche und Erweiterungen von Ringen. Leipzig b. Teubner (1916), S. 57.

§ 5.

Fortgesetzte Betrachtung der allgemeinen algebraischen Erweiterungen.

Wir wollen nun die allgemeinen algebraischen Erweiterungen noch etwas eingehender untersuchen. Dabei müssen wir uns, wie durch ein Beispiel gezeigt werden soll, um zu befriedigenden Ergebnissen zu kommen, ähnlich wie in A. I § 10 auf vollkommene Ringe beschränken.

Satz 11. *Ist $\overline{R}$ eine allgemeine einfache algebraische Erweiterung des vollkommenen Ringes R, so können wir zwischen R und $\overline{R}$ einen Ring $\overline{\overline{R}}$ derart einschalten, daß $\overline{\overline{R}}$ eine regulär algebraische Erweiterung von R darstellt, während $\overline{R}$ aus $\overline{\overline{R}}$ einfach durch Adjunktion eines neuen Primteilers (also durch Adjunktion einer Nullstelle eines zum Primideal $(x, \mathfrak{p}^*)$ gehörigen Primideals) entsteht.*

Ist umgekehrt $\overline{\overline{R}}$ eine regulär algebraische Erweiterung von R und entsteht $\overline{R}$ aus $\overline{\overline{R}}$ durch Adjunktion eines neuen Primteilers, so kann $\overline{R}$ als einfache allgemeine algebraische Erweiterung von R aufgefaßt werden.

Es sei $\overline{R} = R(\alpha)$, wobei α eine Nullstelle des zum Primideal $(g(x), \mathfrak{p}^*)$ gehörigen Primärideals $\mathfrak{a}$ bedeuten möge. Dann ist $g(\alpha)$ ein Nullteiler aus $\overline{R}$, den wir mit $\overline{\mathfrak{p}}$ bezeichnen wollen, es ist mithin α Nullstelle der Funktion $g(x) - \overline{\mathfrak{p}}$ aus $\overline{R}_f$. Es bezeichne nun K den dem Ringe R, $\overline{K}$ den dem Ringe $\overline{R}$ im Sinne von A. I § 6 zugeordneten Körper[24]), $\overline{g}(x)$ bedeute das den modulo $\mathfrak{p}^*$ kongruenten Funktionen $g(x)$ und $g(x) - \overline{\mathfrak{p}}$ zugeordnete Polynom aus K_f. $\overline{g}(x)$ ist in K_f irreduzibel und muß wegen der Vollkommenheit von K im Körper $\overline{K}$, der eine algebraische Erweiterung von K darstellt, in lauter teilerfremde irreduzible Faktoren zerfallen. Daraus ergibt sich nach A. I § 7, daß die Funktionen $g(x)$ und $g(x) - \overline{\mathfrak{p}}$ in $\overline{K}_f$ in teilerfremde Primfunktionen zerfallen müssen, und zwar müssen bei geeigneter Zuordnung entsprechende Primfunktionen der beiden Zerlegungen modulo $\mathfrak{p}_f^*$ kongruent sein. Daraus ergibt sich, daß $g(x)$ in $\overline{R}$ eine mit α modulo $\mathfrak{p}^*$ kongruente Nullstelle α' besitzen muß. α' ist nach Satz 6 hinsichtlich R regulär algebraisch, der Ring $\overline{\overline{R}} = R(\alpha')$ stellt eine reguläre Erweiterung von R dar, und wegen der Kongruenz $\alpha \equiv \alpha'(\mathfrak{p}^*)$ ist den Ringen $\overline{\overline{R}}$ und $\overline{R}$ derselbe Körper $\overline{K}$ zugeordnet, d. h. $\overline{\overline{R}}$ enthält aus jeder Klasse modulo $\mathfrak{p}^*$ kongruenter Elemente von $\overline{R}$ mindestens eines. Adjungieren wir nun zu $\overline{\overline{R}}$ einen beliebigen Primteiler $\overline{\mathfrak{p}}$ aus $\overline{R}$, so kommen wir zu einem Bereiche $\overline{R}'$, dem erstens der Körper $\overline{K}$ zugeordnet ist, und der zweitens aus jeder Klasse äquivalenter Primteiler von $\overline{R}$ mindestens einen Vertreter enthält. Aus diesen

[24]) Also den Körper, der aus R bzw. $\overline{R}$ dadurch entsteht, daß man alle Nullteiler dem Nullelement gleichsetzt.

beiden Tatsachen ergibt sich aber, nach dem in A. I und A. II häufig benutzten „Korrektionsgliederverfahren“[25]), die Identität von $\bar{R}$ und $\bar{R}'$, und hiermit ist der erste Teil von Satz 11 bewiesen.

Zum Beweis des Schlusses nehmen wir an, es sei α ein Element, durch dessen Adjunktion $\bar{R}$ aus R entsteht, während $\bar{p}$ einen Primteiler aus $\bar{R}$ bedeuten möge. Dann ist $\bar{R} = R(\alpha + \bar{p})$. Sicher enthält nämlich $R(\alpha + \bar{p})$ aus jeder Klasse modulo $\mathfrak{p}^*$ kongruenter Elemente von $\bar{R}$ mindestens einen Vertreter. Wir haben also, wie genau wie oben aus dem Korrektionsgliederverfahren folgt, zum Beweise der Gleichung $\bar{R} = R(\alpha + \bar{p})$ nur zu zeigen, daß $R(\alpha + \bar{p})$ einen Primteiler aus $\bar{R}$ enthalten muß. Das ist aber der Fall, wir haben nämlich nach der Taylorentwicklung:

$$g(\alpha + \bar{p}) = g(\alpha) + \bar{p} \cdot g'(\alpha) + \bar{p}^2 \cdot h(\alpha) = \bar{p} \cdot (g'(\alpha) + \bar{p} \cdot h(\alpha)),$$

wobei $g'(x)$ die formal gebildete Ableitung von $g(x)$ bedeutet. Wegen der Vollkommenheit des Ringes R ist nun $g'(x)$ zu $g(x)$ teilerfremd, und es ist daher $g'(\alpha)$, also $g'(\alpha) + \bar{p} \cdot h(\alpha)$ ein reguläres Element aus $\bar{R}$, es stellt mithin $\bar{p} \cdot (g'(\alpha) + \bar{p} \cdot h(\alpha))$ einen in $R(\alpha + \bar{p})$ auftretenden Primteiler dar, und daraus folgt, wie oben bemerkt, die Gleichung $\bar{R} = R(\alpha + \bar{p})$. Der Beweis von Satz 14 ist hiermit abgeschlossen.

Wir wollen noch durch ein Gegenbeispiel zeigen, daß mindestens der erste Teil des Satzes für unvollkommene Ringe seine Gültigkeit verliert. Es sei $R = K_2(t)$ der Körper aller rationalen Funktionen von t mit Koeffizienten modulo 2, und es sei weiter $\bar{R} = R(\alpha)$, wobei α eine Nullstelle des Ideals $((x^2 - t)^2)$ bedeutet. Dann enthält $\bar{R}$ kein hinsichtlich R regulär algebraisches, von den Elementen von R selbst verschiedenes Element. Andernfalls müßte nämlich insbesondere in $\bar{R}$ ein Element $\beta = \sqrt{t}$ vorkommen, das der Gleichung $\beta^2 - t = 0$ genügte[26]), und dieses Element müßte mit α modulo $\mathfrak{p}^*$ kongruent sein, weil ja α modulo $\mathfrak{p}^*$ ebenfalls Nullstelle des Polynoms $x^2 - t$ ist. Bedeutet aber q einen Nullteiler, so haben wir wegen $2 \cdot r_\varepsilon = 0$; $q^2 = 0$ stets $(\alpha + q)^2 = \alpha^2$, und wegen $\alpha^2 - t \neq 0$ kann daher ein Element β von der gewünschten Art in $\bar{R}$ nicht existieren. Bei unvollkommenen Ringen ist es also mitunter unmöglich, zwischen R und $\bar{R}$ einen hinsichtlich R regulär algebraischen Ring $\bar{\bar{R}}$ so einzuschalten, daß $\bar{R}$ aus $\bar{\bar{R}}$ durch Adjunktion eines Primteilers entsteht, Satz 11 verliert seine Gültigkeit.

Wir wenden uns wieder zu vollkommenen Ringen. Der Ring $\bar{R}$ soll als eine allgemeine endliche algebraische Erweiterung des Ringes R be-

---

[25]) Vgl. die Anmerkung bei § 6, wo nochmals von der hier benutzten Schlußweise Gebrauch gemacht wird.

[26]) Dies folgt einfach daraus, daß der dem Ringe $\bar{R}$ zugeordnete Körper $\bar{K}$ aus $R = K$ durch Adjunktion von $\sqrt{t}$ entsteht.

zeichnet werden, wenn $\bar{R}$ aus R durch sukzessive Ausführung von endlich vielen allgemeinen einfachen algebraischen Erweiterungen entsteht. Dann gilt

Satz 12. *Jede allgemeine endliche algebraische Erweiterung eines vollkommenen zerlegbaren Ringes ist einfach.*

Es sei R der Ausgangs-, $\bar{R}$ der Erweiterungsring. Dann genügt es nach dem letzten Teil von Satz 11 zum Beweise von Satz 12, wenn wir zeigen, daß sich zwischen R und $\bar{R}$ ein Erweiterungsring $\bar{\bar{R}}$ so einschalten läßt, daß $\bar{\bar{R}}$ eine einfache regulär algebraische Erweiterung von R darstellt, während $\bar{R}$ aus $\bar{\bar{R}}$ durch Adjunktion eines Primteilers erzeugt werden kann. Wir führen den Beweis dieser Tatsache der Einfachheit halber für den Fall, daß $\bar{R}$ aus R durch zweimalige allgemeine algebraische Erweiterung entsteht. Die Verallgemeinerung auf n-malige Erweiterung ist dann trivial. Es sei also $R^{(1)} = R(\alpha)$; $\bar{R} = R^{(1)}(\beta)$, wobei α ein hinsichtlich R, β ein hinsichtlich $R^{(1)}$ im allgemeinen Sinne algebraisches Element bedeutet. Dann können wir nach Satz 11 zwei Zwischenringe $\bar{\bar{R}}^{(1)}$ und $\bar{\bar{R}}^{(2)}$ so bestimmen, daß $\bar{\bar{R}}^{(1)}$ hinsichtlich R, $\bar{\bar{R}}^{(2)} = R^{(1)}(\beta')$ hinsichtlich $R^{(1)}$ regulär algebraisch ist, und daß $R^{(1)}$ aus $\bar{\bar{R}}^{(1)}$, $\bar{R}$ aus $\bar{\bar{R}}^{(2)}$ jeweils durch Adjunktion eines Primteilers entsteht. Ist nun $g(x)$ diejenige Primfunktion aus $R_f^{(1)}$, deren Nullstelle β' ist, so kann man eine zu $g(x)$ modulo $\mathfrak{p}_f^*$ kongruente Primfunktion $g'(x)$ aus $\bar{\bar{R}}_f^{(1)}$ finden, da ja $\bar{\bar{R}}^{(1)}$ aus jeder Klasse modulo $\mathfrak{p}^*$ kongruenter Elemente von $R^{(1)}$ mindestens eines enthält. Wegen der Vollkommenheit von $R^{(1)}$ und $\bar{\bar{R}}^{(1)}$ folgt nun nach bekannten Schlüssen, daß es in $\bar{\bar{R}}^{(2)}$ eine mit β' modulo $\mathfrak{p}^*$ kongruente Nullstelle β'' von $g'(x)$ gibt und daß β'' hinsichtlich $\bar{\bar{R}}^{(1)}$ regulär algebraisch ist. Der Ring $\bar{\bar{R}} = \bar{\bar{R}}^{(1)}(\beta'')$ ist mithin eine endliche regulär algebraische, also wegen der Vollkommenheit von R eine einfache reguläre Erweiterung von R. Ferner ist dem Ringe $\bar{\bar{R}}$, wie leicht (etwa durch Gradabzählung) einzusehen, derselbe Körper zugeordnet wie dem Ringe $\bar{\bar{R}}^{(2)}$ und folglich wie dem Ringe $\bar{R}$. $\bar{R}$ kann also aus $\bar{\bar{R}}$ durch Adjunktion eines Primteilers gewonnen werden. Hiermit ist, in Anbetracht von Satz 11, Satz 12 für eine zweifache Erweiterung bewiesen, und das Ergebnis läßt sich, wie sofort zu sehen, unmittelbar auf n-fache Erweiterungen übertragen.

Mit dem zuletzt gewonnenen Resultat wollen wir die Betrachtung der allgemeinen endlichen Erweiterungen abschließen. Aus den Sätzen 11 und 12 folgt, daß man, um tiefer in die Natur dieser Erweiterungen einzudringen, sich jedenfalls auf das Studium von solchen Erweiterungsringen beschränken darf, die aus dem Ausgangsring durch Adjunktion eines Primteilers entstehen; denn die regulär algebraischen Erweiterungen eines vollkommenen Ringes wurden ja bereits in A. I § 10 erschöpfend behandelt.

Man könnte auch noch allgemeine unendliche Erweiterungen in Betracht ziehen. Diese dürften in verschiedener Hinsicht von großem Interesse sein, sie führen aber jedenfalls zu Bereichen, die keine zerlegbaren Ringe im Sinne von § 1 mehr sind. Das Studium der allgemeinen unendlichen Erweiterungen fällt daher aus dem der vorliegenden Arbeit gesteckten Rahmen heraus.

§ 6.

Die endlichen zerlegbaren Ringe.

Um sämtliche Typen von endlichen zerlegbaren Ringen zu erhalten, genügt es natürlich, die Typen der speziellen zerlegbaren Ringe aufzustellen, da man ja aus diesen nach der im zweiten Teil entwickelten Methode die allgemeinen ableiten kann.

Was nun die speziellen zerlegbaren Ringe angeht, so ist zunächst zu bemerken, *daß jeder* (*endliche und nicht endliche*) *„Grundring“* [27]) z. zerl. R. *einen zerlegbaren Ring darstellt.* Denn ein Grundring entsteht ja aus dem in evidenter Weise zerlegbaren Ringe der Restklassen nach einer Primzahlpotenz durch regulär algebraische und transzendente Erweiterungen, ist also nach § 3 selbst zerlegbar, und zwar gibt es unter den Vielfachen des Einheitselements einen Primteiler des Grundringes.

vollk. Es handelt sich nun darum, zu untersuchen, wie ein beliebig gegebener spezieller zerlegbarer Ring aus seinem Grundring entsteht. Er ist jedenfalls dann mit seinem Grundring identisch, wenn im Grundring ein Primteiler vorkommt; im anderen Falle kann er aus dem Grundring durch Adjunktion eines Primteilers erzeugt werden. Ist nämlich R_1 ein Teilbereich von R, der den Grundring sowie einen Primteiler von R enthält, so enthält R_1 aus jeder Klasse modulo $\mathfrak{p}^*$ kongruenter Elemente sowie aus jeder Klasse äquivalenter Nullteiler mindestens einen Vertreter und muß daher nach einer im ersten und zweiten Teile verschiedentlich angewandten Schlußweise mit R identisch sein [28]).

Es sei jetzt R ein von seinem Grundring $R^{(1)}$ verschiedener, zerlegbarer Ring, p sei einer seiner Primteiler. Dann muß p hinsichtlich $R^{(1)}$ algebraisch sein und die Adjunktion von p zu $R^{(1)}$ stellt daher eine der in den beiden vorangehenden Paragraphen besprochenen, allgemeinen algebraischen Erweiterungen dar. Die in § 4 und § 5 hergeleiteten Sätze können uns daher sofort zur Aufstellung eines Theorems über die endlichen zerlegbaren Ringe dienen. Wir haben nur die Tatsache zu beachten, daß für die in Satz 8 und Satz 9 auftretende Primfunktion $g(x)$ im vorliegenden Falle x gewählt werden darf, da ja p der Gleichung $p^{\varrho} = 0$ genügt.

---

[27]) Zum Begriffe des Grundringes vgl. A. II § 4 u. 6.

[28]) Vgl. A. I § 10 S. 120, sowie A. II § 7.

Satz 13. *Es sei R ein endlicher, spezieller zerlegbarer Ring, p einer seiner Primteiler, ϱ sein charakteristischer Exponent, während p_0 und ϱ_0 für den zugehörigen Grundring $R^{(1)}$ dieselbe Bedeutung haben. Dann sind folgende Fälle möglich:*

a) $\varrho = \varrho_0$. *In diesem Falle ist $R^{(1)}$ mit R identisch.*

b) $\varrho = \mu \cdot (\varrho_0 - 1) + \nu$ $(\mu > 1;\ 0 < \nu \leqq \mu)$. *In diesem Falle entsteht R aus $R^{(1)}$ durch Adjunktion von p und dasjenige Ideal $\mathfrak{a}$ aus dem zu $R^{(1)}$ gehörigen Funktionenring, dessen Nullstelle p ist, besitzt eine Basis von der Form $(x^\mu + q(x),\ p_0^{\varrho_0 - 1} \cdot x^\nu)$, wobei $q(x)$ für $p_0 \neq 0$ nicht durch p_0^2 teilbar ist.*

c) $\mathfrak{a} = (x^\mu + q(x))$ $\varrho = \mu \varrho_0$.

Ferner ergibt sich aus den Resultaten von § 5 folgender Satz, der in der Theorie der Ideale eines algebraischen Zahlkörpers eine bedeutende Rolle spielt [29]):

Satz 14. *Jeder endliche spezielle zerlegbare Ring kann aus dem (aus den Vielfachen des Einheitselements bestehenden) Primring $R^{(0)}$ durch einfache algebraische Erweiterung gewonnen werden.*

Satz 14 ist eine unmittelbare Folge des zweiten Teils von Satz 12. Denn der Grundring ist ja eine endliche regulär algebraische Erweiterung des Primrings, während R selbst, wie eben festgestellt, aus seinem Grundring durch Adjunktion eines Primteilers entsteht.

Über die Anzahl der Elemente eines endlichen speziellen zerlegbaren Ringes gibt der folgende Satz Aufschluß:

Satz 15. *Ist ϱ der charakteristische Exponent des endlichen speziellen zerlegbaren Ringes R, und gibt es genau π^σ Klassen modulo $\mathfrak{p}^*$ inkongruenter Elemente aus R (π Primzahl)[30]), so enthält R genau $\pi^{\sigma \cdot \varrho}$ Elemente, unter denen sich $\pi^{\sigma \cdot \varrho} \cdot (1 - \pi^{-\sigma})$ reguläre befinden.*

Es bedeute nämlich p einen Primteiler aus R, S einen Bereich, der aus jeder Klasse modulo $\mathfrak{p}^*$ inkongruenter Elemente genau eines enthält. Dann erhält man alle Elemente aus R und jedes nur einmal, wenn man alle Polynome von der Form $\sum\limits_{i=0}^{\varrho-1} a_i p^i$ mit Koeffizienten aus S betrachtet. Ebenso lassen sich alle Nullteiler aus R eindeutig in der Form $\sum\limits_{i=1}^{\varrho-1} a_i p^i$ darstellen.

---

[29]) Vgl. z. B. Hilbert, Die Theorie der algebraischen Zahlkörper. Jahresbericht d. Deutschen Mathematikervereinigung 4 (1897), S. 193.

[30]) Die Anzahl der mod $\mathfrak{p}^*$ inkongruenten Elemente aus R ist sicher eine Primzahlpotenz, sie ist nämlich gleich der Anzahl der Elemente des dem Ringe R zugeordneten endlichen Körpers K.

Jedes reguläre Element aus dem endlichen speziellen zerlegbaren Ringe R genügt der Gleichung $x^{\pi^{\sigma}\cdot\varrho(1-\pi^{-\sigma})} - r_{\varepsilon} = 0$. Doch hat dieses Analogon zum kleinen Fermatschen Satz keine tiefere Bedeutung, da die Funktion $x^{\pi^{\sigma}\cdot\varrho(1-\pi^{-\sigma})} - r_{\varepsilon}$ nur dann Primfunktion ist, wenn R einen Körper darstellt.

Bekanntlich sind zwei endliche Körper isomorph, wenn sie dieselbe Elementezahl besitzen. *Entsprechendes gilt von zwei Grundringen, die in der Anzahl ihrer Elemente und im charakteristischen Exponenten übereinstimmen.* Man könnte vermuten, daß bei den endlichen speziellen zerlegbaren Ringen die Verhältnisse genau so liegen wie bei den Grundringen. Daß dem aber nicht so ist, zeigt das folgende Beispiel.

Als Grundring wählen wir das Restklassensystem modulo 8, und erzeugen aus diesem Grundring durch Adjunktion von $\sqrt{2}$ bzw. $\sqrt{6}$ zwei spezielle zerlegbare Ringe R_1 und R_2 mit den Primteilern $\sqrt{2}$ bzw. $\sqrt{6}$. Wäre nun R_1 zu R_2 isomorph, so müßte R_1 neben $\sqrt{2}$ auch $\sqrt{6}$ enthalten. Das kann aber nicht sein, denn sonst käme in R_1 — da $\sqrt{2}$ und $\sqrt{6}$ Primteiler sind, sich also nur um eine Einheit unterscheiden können — auch $\sqrt{6}:\sqrt{2} = \sqrt{3}$ vor, und das ist, wie leicht einzusehen, unmöglich, weil der Grundring $\sqrt{3}$ nicht enthält, da ja 3 quadratischer Nichtrest nach 8 ist. *R_1 und R_2 sind daher nicht isomorph, trotzdem sie in der Elementezahl und im charakteristischen Exponenten übereinstimmen.*

Als Beispiel für einen endlichen zerlegbaren Ring möge das System S der Restklassen nach einem beliebigen Ideale $\mathfrak{A}$ aus einem algebraischen Zahlkörper betrachtet werden. Zunächst haben wir uns zu überzeugen, daß S tatsächlich einen zerlegbaren Ring darstellt. Das ist der Fall, denn:

1. *S ist ein kommutativer Ring mit Einheitselement.*

2. *S enthält nur endlich viele Elemente, weil es nach $\mathfrak{A}$ nur endlich viele Restklassen gibt. Jedes Element aus S ist daher nach den Ergebnissen von Teil II*[31]) *entweder Einheit oder Nullteiler.*

3. *In S ist jedes Ideal ein Hauptideal, denn nach einem bekannten Satz wird in einem algebraischen Zahlkörper modulo einem festen Ideale jedes andere zum Hauptideal.*

Es sei jetzt $\mathfrak{A} = \prod_{i=1}^{\sigma} \mathfrak{P}_i^{\varrho_i}$, wobei die $\mathfrak{P}_i$ Primideale bedeuten, dann ist eine beliebige Restklasse aus S ein Nullteiler, wenn einer, und folglich jeder ihrer Repräsentanten durch eines der Ideale $\mathfrak{P}_i$ teilbar ist, im andern Fall ist die Restklasse eine Einheit. Zwei Restklassen sind dann und nur dann teilerfremd, wenn nicht die Repräsentanten von beiden gleichzeitig durch eines der Ideale $\mathfrak{P}_i$ teilbar sind. *Aus diesen Tatsachen ergibt sich*

[31]) Vgl. A. II § 4.

leicht, daß die speziellen zerlegbaren Ringe, auf die man S zurückführen kann, durch die Restklassensysteme nach $\mathfrak{P}_1^{\varrho_1}, \mathfrak{P}_2^{\varrho_2}, \ldots, \mathfrak{P}_\sigma^{\varrho_\sigma}$ dargestellt werden.

Wir betrachten also das Restklassensystem R nach der ϱ-ten Potenz eines Primideals $\mathfrak{P}$. Offenbar ist ϱ der charakteristische Exponent von R und ein Element p aus R ist dann und nur dann Primteiler, wenn seine Repräsentanten durch $\mathfrak{P}$, aber nicht durch $\mathfrak{P}^2$ teilbar sind. Um nun zu ermitteln, welcher der in Satz 13 charakterisierten Typen durch R dargestellt wird, beachten wir, daß es eine natürliche Ringzahl π gibt, die durch $\mathfrak{P}$ teilbar ist, und zwar möge $\pi \equiv 0\,(\mathfrak{P}^{\mu})$, $\pi \not\equiv 0\,(\mathfrak{P}^{\mu+1})$ sein. Die durch π repräsentierte Restklasse bezeichnen wir mit p_0. Sie stellt sicher einen Primteiler in dem zu R gehörigen Grundring $R^{(1)}$ dar. Je nach dem Verhältnis der Zahlen μ und ϱ ergeben sich uns folgende Fälle (mit ϱ_0 wird der charakteristische Exponent von $R^{(1)}$ bezeichnet):

a) $\mu = 1$. *In diesem Falle ist R mit seinem Grundring $R^{(1)}$ identisch, denn p_0 stellt einen Primteiler sowohl in $R^{(1)}$ als auch in R dar.*

b) $\mu > 1$. (*Dieser Fall tritt bekanntlich dann und nur dann ein, wenn $\mathfrak{P}$ in der Diskriminante des algebraischen Zahlkörpers, dem es entnommen ist, aufgeht.*) *Setzt man $\varrho = \mu(\varrho_0 - 1) + \nu$ $(0 < \nu \leqq \mu)$, so ist durch diese Gleichung ϱ_0 eindeutig bestimmt, und es stellt den charakteristischen Exponenten von $R^{(1)}$ dar*, wie man sofort erkennt, wenn man sich überlegt, welche Potenz von π unter unsern Voraussetzungen durch $\mathfrak{P}^{\varrho}$ teilbar wird, also verschwindet. — *R entsteht aus $R^{(1)}$ durch Adjunktion von p und $\mathfrak{P}$ ist Nullstelle eines Ideals $(x^{\mu} + q(x),\ p_0^{\varrho_0 - 1} x^{\nu})$ aus $R_f^{(1)}$.*

Da es stets Primideale $\mathfrak{P}$ gibt, die in der Diskriminante ihres Zahlkörpers, also in ihrer Primzahl π in einer höheren als der ersten Potenz aufgehen, so lassen sich, wie man aus der eben durchgeführten Diskussion erkennt, Beispiele für alle die in Satz 11 aufgezählten Fälle bereits unter den Restklassensystemen nach Potenzen von Primidealen aus algebraischen Zahlkörpern finden, der allgemeinste endliche zerlegbare Ring ist also nicht wesentlich komplizierter gebaut als das Restklassensystem nach einem geeignet gewählten algebraischen Ideal. Mit dem eben Festgestellten ist aber noch nicht nachgewiesen, daß sich jeder endliche zerlegbare Ring durch ein derartiges Restklassensystem verkörpern läßt. Um über die Möglichkeit oder Unmöglichkeit einer solchen Darstellung entscheiden zu können, müßte man zunächst folgendes zahlentheoretische Problem lösen:

Es seien $\pi_1, \pi_2, \ldots, \pi_n$ beliebige untereinander verschiedene Primzahlen, σ_{ik}, μ_{ik} $(i = 1, 2, \ldots, n;\ k = 1, 2, \ldots, m_i)$ seien beliebige natürliche Zahlen. Gibt es dann stets einen algebraischen Zahlkörper, in dem für die Primzahlen π_i eine Zerlegung $\pi_i = \prod_{k=1}^{m_i} \mathfrak{P}_k^{\mu_{ik}} \cdot \mathfrak{Q}_i$ gilt, wobei die

$\mathfrak{P}_{ik}$ zueinander und zu $\mathfrak{Q}_i$ teilerfremde Primideale bedeuten, und wobei insbesondere das Restklassensystem nach dem Primideal $\mathfrak{P}_{ik}$ genau $\pi_i^{\sigma_{ik}}$ verschiedene Elemente enthält?)* Läßt sich die aufgeworfene Frage bejahen, so ist damit folgendes gezeigt:

Es seien π_i $(i = 1, 2, \ldots, n)$ beliebige, verschiedene natürliche Primzahlen, σ_{ik}, $\varrho_{ik}^{(0)}$, ϱ_{ik} $(i = 1, 2, \ldots, n;\ k = 1, 2, \ldots, m_i;\ \varrho_{ik} \geqq \varrho_{ik}^{(0)})$ seien beliebige natürliche Zahlen. Dann läßt sich stets ein algebraisches Ideal $\mathfrak{A}$ bestimmen, so daß das Restklassensystem nach $\mathfrak{A}$ einen endlichen zerlegbaren Ring S bildet, der sich als Summe von $\sum\limits_{i=1}^{n} m_i$ speziellen Ringen $R^{(ik)}$ $(i = 1, 2, \ldots, n;\ k = 1, 2, \ldots, m_i)$ darstellen läßt, wobei $R^{(ik)}$ den charakteristischen Exponenten ϱ_{ik} und einen Grundring mit $\pi_i^{\sigma_{ik}}$ verschiedenen Elementen und mit dem Grundringexponenten $\varrho_{ik}^{(0)}$ besitzt.

Bestimmt man nämlich μ_{ik} so, daß die Gleichung

$$\varrho_{ik} = \mu_{ik} \cdot (\varrho_{ik}^{(0)} - 1) + \nu_{ik} \qquad (0 < \nu_{ik} \leqq \mu_{ik})$$

besteht, und sucht man dann einen algebraischen Zahlkörper auf, in dem die Primzahlen π_i in der oben angegebenen Weise in Idealfaktoren zerfallen, so stellt nach dem früher gewonnenen Ergebnis das Restklassensystem nach $\prod\limits_{i=1}^{n} \prod\limits_{k=1}^{m_i} \mathfrak{P}_{ik}^{\varrho_{ik}}$ den gewünschten Ring S dar.

Wäre nun ein endlicher spezieller Ring durch Grundring und charakteristischen Exponenten eindeutig bestimmt, so wäre mit der Lösung des oben formulierten zahlentheoretischen Problems die aufgeworfene Frage erledigt. Da aber, wie gezeigt, zu gegebenem Grundring und charakteristischem Exponenten mitunter mehrere wesentlich verschiedene Ringe existieren, so sind zur vollen Erledigung des vorgelegten Problems noch andere zahlentheoretische Untersuchungen als die oben angegebenen nötig. Hier genügt es, auf den ganzen Fragenkomplex nur hinzuweisen. Denn mit Hilfe von Satz 13 beherrschen wir den Aufbau eines endlichen zerlegbaren Ringes vollständig, wir brauchen daher zur Typisierung dieser Bereiche die Darstellung durch das Restklassensystem nach einem algebraischen Ideal gar nicht.

---

*) Vgl. die während des Druckes erschienene Abhandlung: „*Zur Theorie der Eisensteinschen Gleichungen*" von Herrn Øystein Ore (Math. Zeitschrift 20, S. 267–280), in deren § 4 die hier aufgeworfene Frage für $n = 1$ in bejahendem Sinne beantwortet ist.

§ 7.

Typisierung der allgemeinen vollkommenen zerlegbaren Ringe.

Zum Abschluß der vorliegenden Arbeit sollen noch einige Bemerkungen über die Typisierung von beliebigen vollkommenen zerlegbaren Ringen gemacht werden. Da bei einem vollkommenen Ringe die Existenz des Grundrings nach den Resultaten von A II feststeht, so können wir sagen:

Satz 13a. *Jeder vollkommene zerlegbare Ring kann aus seinem Grundring in derselben Weise wie ein endlicher zerlegbarer Ring durch allgemeine algebraische Erweiterung erzeugt werden.*

Mit Hilfe von Satz 13a können wir den Aufbau der vollkommenen zerlegbaren Ringe in genau der gleichen Weise übersehen wie den der endlichen Ringe.

Es sollen nun noch einige weitergehende Untersuchungen angestellt werden, die sich vorwiegend auf algebraisch abgeschlossene Ringe beziehen. Dabei wollen wir folgende Ausdrucks- und Schreibweise gebrauchen:

Es sei R der gegebene Ring. Dann bezeichnet $R^{(1)}$ seinen Grundring, ϱ den charakteristischen Exponenten von R, $\varrho^{(1)}$ denjenigen von $R^{(1)}$, den „Grundringexponenten". Ist $R^{(1)}$ kein Körper, gibt es also eine Primzahl π, so daß das Element $\pi \cdot r_\varepsilon$ einen von Null verschiedenen Primteiler aus $R^{(1)}$ darstellt, so soll π als „kritische Primzahl" von R bezeichnet werden. Für das Element $\pi \cdot r_\varepsilon$ wollen wir alsdann stets die Schreibweise p_1 benutzen, während $p, p', \ldots$ Primteiler aus R selbst bedeuten sollen. Als „kritische Invariante" μ des Ringes R bezeichnen wir schließlich die durch die Gleichung $\varrho = (\varrho_1 - 1) \cdot \mu + \nu$ $(0 < \nu \leqq \mu)$ eindeutig bestimmte positive Zahl μ.

Wir gehen jetzt zur Behandlung der Isomorphiefrage bei vollkommenen zerlegbaren Ringen über. Natürlich ist, wie das im vorangehenden Paragraphen gegebene Beispiel zeigt, ein vollkommener Ring durch Grundring und charakteristischen Exponenten nicht eindeutig bestimmt. Doch sind zwei wichtige Fälle hervorzuheben, bei denen die Sache anders liegt.

Satz 16. *Ein vollkommener zerlegbarer Ring, dessen Grundring ein Körper ist, ist durch Grundring und charakteristischen Exponenten bis auf Isomorphie eindeutig bestimmt.*

Der eben formulierte Satz ist beinahe trivial, da nach Satz 13a ein vollkommener Ring R, dessen Grundring $R^{(1)}$ ein Körper ist, aus $R^{(1)}$ durch Adjunktion einer Nullstelle des Ideals (x^ϱ) entsteht. Zu einem interessanteren

Falle gelangen wir, wenn wir algebraisch abgeschlossene Ringe betrachten. Es ist natürlich in Anbetracht von Satz 16 nur der Fall zu untersuchen, in dem der Grundring kein Körper ist.

Satz 17. *Es sei R ein algebraisch abgeschlossener zerlegbarer Ring. Dann ist R in folgenden Fällen durch Grundring und charakteristischen Exponenten eindeutig bestimmt:*

α) *Wenn $R^{(1)}$ ein Körper ist.*

β) *Wenn die kritische Invariante μ zur kritischen Primzahl π teilerfremd ist.*

γ) *Wenn $\varrho = \mu + 1$; $\varrho_1 = 2$ ist.*

In allen übrigen Fällen kann man stets zwei nicht isomorphe Ringe mit gleichem Grundring und gleichem charakteristischen Exponenten angeben.

α) ist bereits durch Satz 16 erledigt. In den Fällen β) und γ) führt uns der Nachweis zum Ziel, daß wir R stets aus $R^{(1)}$ durch Adjunktion einer Nullstelle p des Ideals $(x^{\mu} - p_1,\ x^{\nu} \cdot p_1^{\varrho_1 - 1})$ erhalten können, denn das angeschriebene Ideal ist ja nur vom Grundring und von der kritischen Invariante, also wegen des Zusammenhangs zwischen μ und ϱ nur von $R^{(1)}$ und von ϱ abhängig. Um das Element p in der gewünschten Weise zu bestimmen, betrachte man einen beliebigen Primteiler p' aus R. p' ist Nullstelle eines Ideals $(x^{\mu} - p_1 \cdot f(x),\ x^{\nu} \cdot p_1^{\varrho_1 - 1})$ aus $R_f^{(1)}$, wobei $f(p')$ ein reguläres Element aus R bedeutet. Ist nun μ zur kritischen Primzahl π teilerfremd, so zerfällt in dem dem Ringe R zugeordneten, algebraisch abgeschlossenen Körper K die Funktion $x^{\mu} - \overline{f(p')}$ in lauter teilerfremde Linearfaktoren, und es gilt daher nach A I § 6 das gleiche von dem Polynom $x^{\mu} - f(p')$ aus R_f. Wir können infolgedessen ein reguläres Element a aus R so wählen, daß es der Gleichung $x^{\mu} - f(p') = 0$ genügt. Setzt man $p' = p \cdot a$, so ist $p = p' \cdot a^{-1}$ ebenfalls ein Primteiler, und zwar ein solcher, der die Gleichung $x^{\mu} - p_1 = 0$ befriedigt. Das Ideal, dessen Nullstelle p ist, besitzt daher die gewünschte Basis $(x^{\mu} - p_1,\ x^{\nu} \cdot p_1^{\varrho_1 - 1})$. Etwas anders muß man im Falle γ) schließen. Hier verschwindet das Produkt von p_1 mit einem beliebigen Nullteiler aus R, und das Ideal, dessen Nullstelle p' ist, besitzt daher eine Basis $(x^{\mu} - a \cdot p_1,\ p_1 \cdot x)$, wobei a ein modulo $\mathfrak{p}^*$ beliebig wählbares Element aus R bedeutet. Wegen der algebraischen Abgeschlossenheit von R darf man alsdann a so gewählt annehmen, daß die Gleichung $x^{\mu} - a = 0$ in R eine Nullstelle a_1 besitzt. Setzt man $p' = p \cdot a_1$, so ist p eine der gesuchten Nullstellen des Ideals $(x^{\mu} - p_1,\ x \cdot p_1)$. Die Fälle β) und γ) sind hiermit erledigt.

Es bleibt nur noch zu zeigen, daß für $\varrho \neq \mu + 1$; $\varrho_1 \geqq 2$ stets zu einem gegebenen Grundring mit der kritischen Primzahl π zwei nicht isomorphe Ringe mit derselben kritischen, zu π nicht teilerfremden Invariante μ aufgebaut werden können. Wir setzen $\mu = \pi^{\sigma} \cdot \mu'$; $(\mu', \pi) = 1$ und betrachten die Ideale

$$\mathfrak{a} = (x^{\mu} - p_1,\ p_1^{\varrho_1 - 1} \cdot x^{\nu}) \quad \text{und} \quad \mathfrak{a}' = (x^{\mu} - p_1 \cdot (x + r_{\varepsilon}),\ p_1^{\varrho_1 - 1} \cdot x^{\nu}).$$

Es sei p eine Nullstelle von $\mathfrak{a}$, p' eine solche von $\mathfrak{a}'$;

$$R = R^{(1)}(p), \qquad R' = R^{(1)}(p').$$

Dann können R und R' nicht isomorph sein.

Andernfalls müßte nämlich R ebenso wie R' eine Nullstelle des Ideals $\mathfrak{a}'$ enthalten, die wir der Einfachheit halber gleichfalls mit p' bezeichnen wollen. Da p und p' Primteiler sind, so besteht eine Gleichung $p' = a \cdot p$. Wir haben also $a^{\mu} \cdot p^{\mu} - p_1 \cdot (p' + r_{\varepsilon}) = (a^{\mu} - (p' + r_{\varepsilon})) \cdot p_1 = 0$. Setzen wir mithin $a^{\mu} = r_{\varepsilon} + p' + q$, so muß q der Gleichung $q \cdot p_1 = 0$ genügen, und daraus ergibt sich wegen $\varrho_1 \geqq 2$; $\varrho > \mu + 1$, daß q mindestens durch p'^2 teilbar sein muß, wir haben also $a^{\mu} = r_{\varepsilon} + p' \cdot r$, wobei r eine Einheit bedeutet. Wir betrachten nun die Differenz $s = r_{\varepsilon} - a^{\mu'}$. Es ist

$$s^{\pi^{\sigma}} = r_{\varepsilon} + (-1)^{\pi^{\sigma}} \cdot a^{\mu} + p_1 \cdot b = r_{\varepsilon} \cdot (1 + (-1)^{\pi^{\sigma}}) + (-1)^{\pi^{\sigma}} p' \cdot r + p_1 \cdot b.$$

Da nun $r_{\varepsilon} \cdot (1 + (-1)^{\pi^{\sigma}}) = \begin{cases} p_1 \ (\pi = 2) \\ 0 \ \ (\pi = 2) \end{cases}$ ebenso wie $p_1 \cdot b$ mindestens durch p'^2 teilbar ist, so ist $s^{\pi^{\sigma}} = (-1)^{\pi^{\sigma}} p'(r + p' \cdot c) = p' \cdot r_1$ das Produkt eines Primteilers mit einer Einheit, also selbst Primteiler. Enthielte mithin R gleichzeitig die Elemente p und p', so müßte es in R ein Element s geben, das π^{σ}-te Wurzel eines Primteilers wäre[32]). Da die Existenz eines solchen Elementes der Natur des Primteilers widerspricht, so kann p' nicht in R vorkommen, R und R' sind also nicht isomorph. Mit dem so gewonnenen Ergebnis ist der Beweis unseres Satzes abgeschlossen.

Aus Satz 17 ergibt sich, daß man zwei isomorphe Ringe erhält, wenn man die bei Besprechung der endlichen Ringe aufgebauten nicht isomorphen Bereiche $R(\sqrt{2})$ und $R(\sqrt{6})$ zu algebraisch abgeschlossenen Ringen ergänzt. Es ist also, wenn zwei nicht isomorphe Ringe mit gleichem Grundring und gleicher kritischer Invariante vorgelegt sind, wohl zu unterscheiden,

---

[32]) Man vergleiche das hier gegebene Beispiel mit dem am Schlusse von A. I angegebenen, durch das bewiesen wurde, daß bei unvollkommenen Ringen zwei regulär algebraische Erweiterungen desselben Ausgangsringes mit gleichem zugeordneten Körper nicht stets äquivalent sind. Die hier und dort benutzten Schlüsse laufen ganz parallel. Die aus der kritischen Primzahl entspringenden Schwierigkeiten sind in beiden Fällen im ganzen dieselben. Der einzige wesentliche Unterschied ist der, daß hier die Primteiler eine analoge Rolle spielen, wie in A. I die transzendenten Elemente.

ob der Grund für die Nichtisomorphie an der algebraischen Natur des Grundrings liegt, oder ob wir es mit einer Nichtisomorphie zu tun haben, die mit der kritischen Primzahl zusammenhängt, und durch regulär algebraische Erweiterung nicht behoben werden kann.

Im Anschluß an Satz 17 kann man sich noch folgende Frage vorlegen. Es seien R und R' zwei algebraisch abgeschlossene, nicht isomorphe Ringe, mit gleichem Grundring und gleichem charakterischen Exponenten. Wann kann man dann die Nichtisomorphie durch allgemeine algebraische Erweiterung beheben, d. h. wann kann man einen Ring $\overline{R}$ finden, der sowohl einen zu R als auch einen zu R' isomorphen Teilbereich enthält, und der sich als allgemeine algebraische Erweiterung von R (bzw. von R') auffassen läßt?

Die hier aufgeworfene Frage hängt, wie leicht zu sehen[33]), mit folgendem Problem aufs engste zusammen:

Es sei $h(x)$ eine Primärfunktion μ-ten Grades aus R_f, von der wir wegen der algebraischen Abgeschlossenheit von R ohne wesentliche Beschränkung voraussetzen dürfen, daß sie zum Primideal (x, p) gehört. Wann enthält dann R eine Nullstelle von $h(x)$ und wann kann man eine allgemeine algebraische Erweiterung $\overline{R}$ von R derart bestimmen, daß $h(x)$, wenn auch nicht in R, so doch in $\overline{R}$ eine Nullstelle besitzt?

Die eben gestellte Frage bedeutet in gewissem Sinne eine Verallgemeinerung des Problems, das uns zur Einführung der allgemeinen algebraischen Erweiterungen hinleitete. Dort betrachteten wir eine Primärfunktion $h(x)$, die nicht durch das Quadrat des zugehörigen Primideals teilbar war, und stellten fest, daß man einfach durch Adjunktion einer Nullstelle von $h(x)$ zum gewünschten Erweiterungsring kommt (falls nicht $h(x)$ bereits im Ausgangsring eine Nullstelle besitzt). Im allgemeinen Falle liegt die Sache verwickelter. Da würde die Adjunktion einer Nullstelle von $h(x)$ selbst im allgemeinen zu einem Erweiterungsring führen, der

[33]) Man vergleiche das beim Beweise von Satz 17 angeführte Beispiel von zwei nicht isomorphen Ringen R und R'. Dort wurde gezeigt: In einem Ring $\overline{R}$, der gleichzeitig einen zu R und einen zu R' isomorphen Teilbereich enthält, muß die π^σ-te Wurzel eines gewissen, zu einem Primteiler aus R äquivalenten Elementes vorkommen. Das heißt aber nichts anderes, als daß eine gewisse, zum Primideal (x, p) gehörige Primärfunktion π^σ-ten Grades aus R_f in $\overline{R}$ eine Nullstelle besitzen muß. Dabei ist in unserem besonderen Falle die in Betracht kommende Primärfunktion $h(x)$ nicht durch das Quadrat des Primideals (x, p) teilbar. Man kann hier also $\overline{R}$ unmittelbar durch Adjunktion einer Nullstelle von $h(x)$ aus R erzeugen. Der so aufgebaute Ring $\overline{R}$ enthält dann, wie leicht zu sehen, wirklich einen zu R' isomorphen Teilbereich, in diesem besonderen Falle kann man also die Nichtisomorphie von R und R' sicher durch algebraische Erweiterung heben. Nicht so einfach gestaltet sich, wie oben betont, die Sache im allgemeinen Fall.

nicht mehr zerlegbar wäre. Gleichwohl erscheint es durchaus nicht ausgeschlossen, daß man durch Adjunktion einer Nullstelle einer anderen, geeignet gewählten Primärfunktion einen Erweiterungsring der gewünschten Art aufbauen könnte. Doch dürfte die allgemeine Beantwortung der aufgeworfenen Frage nicht einfach sein. Wir müssen uns daher hier mit dem Hinweis begnügen, daß die Einführung der allgemeinen algebraischen Erweiterungen auf eine Reihe von interessanten, einer ausführlichen Behandlung wohl würdigen Problemen hinleitet.

Für die vorliegende Arbeit reichen die mit Satz 13a und Satz 17 gewonnenen Ergebnisse vollständig aus. Satz 13a leistet für die vollkommenen zerlegbaren Ringe dasselbe wie Satz 13 für die endlichen: er gibt uns einen befriedigenden Einblick in diese Bereiche. Satz 17 hingegen charakterisiert in erschöpfender Weise diejenigen Fälle, in denen sich ein vollkommener Ring durch Grundring und charakteristischen Exponenten eindeutig bestimmen läßt. Am interessantesten ist dabei die Erkenntnis von der großen Bedeutung, die die kritische Primzahl für den Aufbau der zerlegbaren Ringe besitzt. Hier zeigt sich am schärfsten der Zusammenhang mit der Körpertheorie (vgl. die Bemerkung am Schlusse der Einleitung), der die in der vorliegenden Arbeit durchgeführte algebraische Behandlung der zerlegbaren Ringe rechtfertigt.

(Eingegangen am 31. 12. 1923.)