Idealtheorie in Ringbereichen.

Von

Emmy Noether in Göttingen.

Inhaltsverzeichnis.

Einleitung.

Den Inhalt der vorliegenden Arbeit bildet die *Übertragung der Zerlegungssätze der ganzen rationalen Zahlen, bzw. der Ideale in algebraischen Zahlkörpern, auf Ideale in beliebigen Integritäts-, allgemeiner Ringbereichen.* Zum Verständnis dieser Übertragung seien vorerst für die ganzen rationalen Zahlen die Zerlegungssätze etwas abweichend von der üblichen Formulierung angegeben.

Faßt man in

$$a = p_1^{\varrho_1} p_2^{\varrho_2} \dots p_\sigma^{\varrho_\sigma} = q_1 q_2 \dots q_\sigma$$

die Primzahlpotenzen q_i als Komponenten der Zerlegung auf, so kommen diesen Komponenten die folgenden charakteristischen Eigenschaften zu:

1. Sie sind *paarweise teilerfremd*; aber kein q ist als Produkt paarweise teilerfremder Zahlen darstellbar, also besteht in diesem Sinne Irreduzibilität. Aus der paarweisen Teilerfremdheit folgt noch, daß das Produkt $q_1 \dots q_\sigma$ gleich dem kleinsten gemeinsamen Vielfachen $[q_1 \dots q_\sigma]$ wird.

2. Je zwei der Komponenten, q_i und q_k, sind *relativprim*; d. h. ist $b \cdot q_i$ durch q_k teilbar, so ist b durch q_k teilbar. Auch in diesem Sinne besteht Irreduzibilität.

3. Jedes q ist *primär*; d. h. ist ein Produkt $b \cdot c$ durch q teilbar, aber b nicht teilbar, so ist eine Potenz [1]) von c teilbar. Die Darstellung ist ferner eine solche durch *größte primäre Komponenten*, da das Produkt zweier verschiedener q nicht mehr primär ist. Auch in bezug auf die Zerlegung in größte primäre Komponenten sind die q irreduzibel.

4. Jedes q ist *irreduzibel* in dem Sinne, daß es sich nicht als kleinstes gemeinsames Vielfaches von zwei echten Teilern darstellen läßt.

Der Zusammenhang dieser primären Zahlen q mit den Primzahlen p besteht darin, daß es zu jedem q ein und (vom Vorzeichen abgesehen) nur ein p gibt, das Teiler von q ist und von dem eine Potenz durch q teilbar ist: die zugehörige Primzahl. Ist p^ϱ die niedrigste derartige Potenz — ϱ der Exponent von q —, so wird hier insbesondere p^ϱ gleich q. Der *Eindeutigkeitssatz* läßt sich nun so aussprechen:

Bei zwei verschiedenen Zerlegungen einer ganzen rationalen Zahl in die irreduziblen, größten primären Komponenten q stimmen die Anzahl der Komponenten, die zugehörigen Primzahlen (bis auf das Vorzeichen) und die Exponenten überein. Wegen $p^\varrho = q$ folgt hieraus auch das Übereinstimmen der q selbst (bis auf das Vorzeichen).

---

[1]) Ist diese Potenz stets die erste, so handelt es sich bekanntlich um Primzahlen.

Die durch das Vorzeichen gegebene Unbestimmtheit wird bekanntlich aufgehoben, wenn man statt der Zahlen die aus ihnen abgeleiteten Ideale (alle durch a teilbaren Zahlen) betrachtet; dann gilt die Formulierung genau so für die eindeutige Zerlegung der Ideale der (endlichen) algebraischen Zahlkörper in Primidealpotenzen.

Im folgenden wird nun (§ 1) ein allgemeiner Ringbereich zugrunde gelegt, der nur der *Endlichkeitsbedingung* genügen muß, daß jedes Ideal des Bereichs eine endliche Idealbasis besitzt. Ohne eine solche Endlichkeitsbedingung brauchten nämlich keine irreduziblen und Prim-Ideale zu existieren, wie der Bereich *aller* ganzen algebraischen Zahlen zeigt, in dem es keine Zerlegung in Primideale gibt.

Es zeigt sich, daß — entsprechend den vier charakteristischen Eigenschaften der Komponenten q — im allgemeinen *vier getrennte Zerlegungen existieren, die jeweils durch Unterspaltung auseinander hervorgehen.* Dabei handelt es sich bei der Zerlegung in teilerfremd-irreduzible Ideale um eine Produktdarstellung, bei den übrigen drei Zerlegungen um eine reduzierte (§ 2) Darstellung als kleinstes gemeinsames Vielfaches. Auch der Zusammenhang zwischen primärem Ideal — auch die irreduziblen Ideale sind primär — und zugehörigem Primideal bleibt erhalten: Zu jedem primären Ideal $\mathfrak{Q}$ ist eindeutig ein zugehöriges Primideal $\mathfrak{P}$ bestimmt, das Teiler von $\mathfrak{Q}$ ist, und von dem eine Potenz durch $\mathfrak{Q}$ teilbar wird. Ist $\mathfrak{P}^\varrho$ die niedrigste derartige Potenz — ϱ der Exponent von $\mathfrak{Q}$ —, so braucht aber hier $\mathfrak{P}^\varrho$ nicht mit $\mathfrak{Q}$ übereinzustimmen. Der *Eindeutigkeitssatz* spricht sich nun so aus:

Die Zerlegungen 1 *und* 2 *sind eindeutig; bei zwei verschiedenen Zerlegungen* 3 *oder* 4 *stimmen die Anzahl der Komponenten und die zugehörigen Primideale überein*[2]*; die unter den Komponenten auftretenden isolierten Ideale* (§ 7) *sind eindeutig bestimmt.*

Zum Beweise der Zerlegungssätze wird aus der Endlichkeitsbedingung der zuerst von Dedekind für endliche Zahlenmoduln ausgesprochene „Satz von der endlichen Kette“ gefolgert und daraus die Darstellung 4 eines jeden Ideals als kleinstes gemeinsames Vielfaches von endlich vielen irreduziblen Idealen abgeleitet. Durch Umformung des Begriffs der Reduzibilität einer Komponente ergibt sich daraus der grundlegende *Eindeutigkeitssatz für die Zerlegung* 4 *in irreduzible Ideale.* Durch Zusammenfassen von je endlich vielen Komponenten wird zu den übrigen Zerlegungen aufgestiegen, deren Eindeutigkeitssätze sich als Folge von Eindeutigkeitssatz 4 ergeben.

---

[2]) Vermutlich gilt darüber hinaus auch das Übereinstimmen der Exponenten, und noch allgemeiner die Isomorphie entsprechender Komponenten.

Schließlich wird gezeigt (§ 9), daß die Darstellung durch endlich viele *irreduzible* Komponenten auch unter geringeren Voraussetzungen statthat; die Kommutativität des Ringbereiches ist nicht erforderlich, und es genügt, an Stelle eines Ideals einen Modul in bezug auf den Bereich zu betrachten. In diesem allgemeineren Fall gilt noch die *Anzahlgleichheit der Komponenten* bei zwei verschiedenen Zerlegungen, während die Begriffe prim und primär an Kommutativität und Idealbegriff gebunden sind; dagegen bleibt der Begriff teilerfremd bei Idealen in nichtkommutativen Bereichen erhalten.

Der einfachste Ringbereich, für den tatsächlich die vier getrennten Zerlegungen auftreten, ist der Bereich aller Polynome von n Variablen mit beliebigen komplexen Koeffizienten. Die einzelnen Zerlegungen lassen sich hier irrational durch das Verhalten der algebraischen Gebilde deuten, und der Eindeutigkeitssatz für die zugehörigen Primideale entspricht dem Fundamentalsatz der Eliminationstheorie von der eindeutigen Zerlegbarkeit der algebraischen Gebilde in irreduzible. Weitere Beispiele sind gegeben durch alle endlichen Integritätsbereiche aus Polynomen (§ 10). Aber auch der einfache Bereich aller geraden Zahlen, allgemeiner aller durch eine feste Zahl teilbaren Zahlen, bietet schon ein Beispiel von teilweise getrennten Zerlegungen (§ 11). Ein Beispiel der Idealtheorie in nichtkommutativen Bereichen liefert die Elementarteilertheorie (§ 12), wo eindeutige Zerlegung in irreduzible Ideale, bzw. Klassen besteht. Diese irreduziblen Klassen charakterisieren vollständig die irreduziblen Bestandteile der Elementarteiler, können vielleicht für Bereiche, wo die gewöhnliche Elementarteilertheorie versagt, als deren Äquivalent angesehen werden.

Über die vorhandene Literatur ist das Folgende zu bemerken: Die Zerlegung in *größte primäre Ideale* ist für den Polynombereich mit beliebigen komplexen bzw. ganzzahligen Koeffizienten von Lasker gegeben, von Macaulay in einzelnen Punkten weitergeführt[3]). Beide stützen sich auf die Eliminationstheorie, benutzen also die Tatsache, daß ein Polynom sich eindeutig als Produkt von irreduziblen Polynomen darstellen läßt. Tatsächlich sind die Zerlegungssätze für Ideale von dieser Voraussetzung unabhängig, wie die Idealtheorie in algebraischen Zahlkörpern vermuten läßt und wie die vorliegende Arbeit zeigt. Auch das primäre Ideal ist bei Lasker und Macaulay unter Zugrundelegung von Begriffen aus der Eliminationstheorie definiert.

Die Zerlegung in *irreduzible* Ideale und die in *relativprim-irreduzible*

[3]) E. Lasker, Zur Theorie der Moduln und Ideale. Math. Ann. **60** (1905), S. 20, Satz VII und XIII. — F. S. Macaulay, On the Resolution of a given Modular System into Primary Systems including some Properties of Hilbert Numbers. Math. Ann. **74** (1913), S. 66.

scheint in der Literatur auch für den Polynombereich nicht bemerkt; nur bei Macaulay findet sich eine Bemerkung über die Eindeutigkeit der isolierten primären Ideale.

Die Zerlegung in *teilerfremd-irreduzible* Ideale ist für den Polynombereich von Schmeidler[4]) gegeben, unter Benutzung der Eliminationstheorie für den Endlichkeitsnachweis. Doch ist hier der Eindeutigkeitssatz nur für Klassen von Idealen, nicht für die Ideale selbst ausgesprochen. Dieser letztere Eindeutigkeitssatz findet sich in einer gemeinsamen Arbeit[5]), wo es sich um Ideale in nichtkommutativen Polynombereichen handelt. Hier wird nur von der endlichen Idealbasis Gebrauch gemacht, Sätze und Methoden bleiben also für allgemeine Ringbereiche bestehen, lassen sich durch die vorliegende Arbeit in bezug auf die Anzahlgleichheit verschärfen (§ 11). Die vorliegenden Untersuchungen stellen eine starke Verallgemeinerung und Weiterentwicklung der diesen beiden Arbeiten zugrunde liegenden Begriffsbildungen dar. Das Wesentliche der beiden Arbeiten ist der Übergang von der Darstellung als kleinstes gemeinsames Vielfaches zu einer additiven Zerlegung des Systems der Restklassen. Hier wird der einfacheren Darstellung halber wieder beim kleinsten gemeinsamen Vielfachen geblieben; der additiven Zerlegung entspricht dann die Umformung des Begriffs der Reduzibilität in eine Eigenschaft des Komplements (§ 3). Doch lassen sich nach Überlegungen, die wesentlich denen der gemeinsamen Arbeit entsprechen, alle angegebenen Sätze auch als additive Zerlegungssätze für das System der Restklassen und gewisser Teilsysteme auffassen. Dieses System der Restklassen bildet einen Ring von gleicher Allgemeinheit wie der ursprünglich zugrunde gelegte; es kann nämlich jeder Ring aufgefaßt werden als System der Restklassen desjenigen Ideals, das der Gesamtheit der identischen Relationen zwischen den Ringelementen entspricht; oder auch einem Teilsystem dieser Relationen, indem man die übrigen Relationen auch im Bereich als erfüllt annimmt.

Diese Bemerkung gibt auch die Einordnung der Arbeiten von Fraenkel[6]). Fraenkel betrachtet additive Zerlegungen von Ringen, die solchen einschränkenden Bedingungen unterworfen werden (Existenz regulärer Elemente, Division durch diese, Zerlegbarkeitsbedingung), daß für das ent-

---

[4]) W. Schmeidler, Über Moduln und Gruppen hyperkomplexer Größen. Math. Zeitschr. **3** (1919), S. 29.

[5]) E. Noether-W. Schmeidler, Moduln in nichtkommutativen Bereichen, insbesondere aus Differential- und Differenzenausdrücken. Math. Zeitschr. 8 (1920), S. 1.

[6]) A. Fraenkel, Über die Teiler der Null und die Zerlegung von Ringen. J. f. M. **145** (1914), S. 139. Über gewisse Teilbereiche und Erweiterungen von Ringen. Habilitationsschrift, Leipzig, Teubner, 1916. Über einfache Erweiterungen zerlegbarer Ringe. J. f. M. **151** (1920), S. 121.

sprechende Ideal die vier Zerlegungen zusammenfallen. Wegen dieses Zusammenfallens bedeutet auch seine Endlichkeitsbedingung, daß das Ideal nur endlich viele echte Teiler besitzen soll — von der übrigens teilweise abgesehen wird —, keine stärkere Einschränkung als unsere. Der Ausgangspunkt Fraenkels ist durch die andersartigen, im wesentlichen algebraischen Ziele seiner Arbeiten bedingt; durch algebraische Erweiterung gelangt er dann zu allgemeineren Ringen mit weniger einschränkenden Bedingungen.

§ 1.

Ringbereich, Ideal, Endlichkeitsbedingung.

1. Der zugrunde gelegte Bereich Σ sei ein (kommutativer) *Ring* in abstrakter Definition[7]); d. h. Σ bestehe aus einem System von Elementen $a, b, c, \ldots, f, g, h, \ldots$, in dem eine den üblichen Bedingungen genügende Relation als *Gleichheit* definiert ist; und in dem durch zwei Operationen (Verknüpfungsarten), *Addition* und *Multiplikation*, aus je zwei Ringelementen a und b stets eindeutig je ein drittes als Summe $a+b$ und als Produkt $a \cdot b$ gewonnen wird. Der Ring und die sonst ganz willkürlichen Operationen müssen dabei den folgenden Gesetzen genügen:

1. *Dem assoziativen Gesetz der Addition*: $(a+b)+c=a+(b+c)$.
2. *Dem kommutativen Gesetz der Addition*: $a+b=b+a$.
3. *Dem assoziativen Gesetz der Multiplikation*: $(a\cdot b)\cdot c=a\cdot(b\cdot c)$.
4. *Dem kommutativen Gesetz der Multiplikation*: $a\cdot b=b\cdot a$.
5. *Dem distributiven Gesetz*: $a\cdot(b+c)=a\cdot b+a\cdot c$.
6. *Dem Gesetz der unbeschränkten und eindeutigen Subtraktion.*

Es gibt in Σ ein einziges Element x, das die Gleichung $a+x=b$ befriedigt. (Man bezeichnet $x=b-a$.)

Aus diesen Eigenschaften folgt die Existenz der Null; ein Ring braucht aber keine Einheit zu besitzen; und es kann das Produkt zweier Elemente verschwinden, ohne daß ein Faktor verschwindet. Ringe, für die aus dem Verschwinden eines Produktes stets das Verschwinden eines Faktors folgt, und die außerdem eine Einheit besitzen, werden als *eigentliche Integritätsbereiche* bezeichnet. Für die endliche Summe $a+a\ldots+a$ führen wir die übliche abkürzende Bezeichnung na ein, wobei die ganzen Zahlen n lediglich als abkürzende Zeichen, nicht als Ringelemente zu betrachten sind, und durch $a=1\cdot a$, $na+a=(n+1)a$ rekurrierend definiert sind.

---

[7]) Die Definition ist der Fraenkelschen Habilitationsschrift entnommen, unter Weglassung dessen einschränkender Bedingungen 6, I und II; dafür mußte das kommutative Gesetz der Addition mit aufgenommen werden. Es handelt sich also um die den Körper definierenden Gesetze unter Weglassung der Umkehrbarkeit der Multiplikation.

2. Unter einem *Ideal* $\mathfrak{M}$[8]) in Σ werde ein System von Elementen aus Σ verstanden, das den beiden Bedingungen genügt:

1. $\mathfrak{M}$ *enthält neben* f *auch* $a \cdot f$, *wo* a *ein beliebiges Element aus* Σ *ist.*

2. $\mathfrak{M}$ *enthält neben* f *und* g *auch die Differenz* $f-g$; also neben f auch nf für jede ganze Zahl n.

Ist f Element von $\mathfrak{M}$, so drücken wir das wie üblich durch $f \equiv 0\,(\mathfrak{M})$ aus; und sagen, f *ist durch* $\mathfrak{M}$ *teilbar.* Ist jedes Element von $\mathfrak{N}$ zugleich Element von $\mathfrak{M}$, also teilbar durch $\mathfrak{M}$, so sagen wir: $\mathfrak{N}$ *ist durch* $\mathfrak{M}$ *teilbar*; in Zeichen: $\mathfrak{N} \equiv 0\,(\mathfrak{M})$. $\mathfrak{M}$ heißt *echter Teiler* von $\mathfrak{N}$, wenn es von $\mathfrak{N}$ verschiedene Elemente enthält, also nicht umgekehrt durch $\mathfrak{N}$ teilbar ist. Aus $\mathfrak{N} \equiv 0\,(\mathfrak{M})$; $\mathfrak{M} \equiv 0\,(\mathfrak{N})$ folgt $\mathfrak{N} = \mathfrak{M}$.

Auch die übrigen bekannten Begriffe bleiben wörtlich erhalten. Unter dem *größten gemeinsamen Teiler* zweier Ideale $\mathfrak{A}$ und $\mathfrak{B}$ — $\mathfrak{D} = (\mathfrak{A}, \mathfrak{B})$ — verstehen wir die Gesamtheit der Elemente, die sich in der Form $a+b$ darstellen lassen, wo a alle Elemente aus $\mathfrak{A}$, b alle aus $\mathfrak{B}$ durchläuft; $\mathfrak{D}$ wird wieder ein Ideal. Ebenso ist der größte gemeinsame Teiler von unendlich vielen Idealen — $\mathfrak{D} = (\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_\nu, \ldots)$ — definiert als Gesamtheit der Elemente d, die sich darstellen lassen als Summe der Elemente von jeweils endlich vielen Idealen: $d = a_{i_1} + a_{i_2} + \ldots + a_{i_n}$; auch hier wird $\mathfrak{D}$ wieder ein Ideal.

Enthält das Ideal $\mathfrak{M}$ insbesondere eine endliche Anzahl von Elementen $f_1, f_2, \ldots, f_\varrho$ derart, daß

$$\mathfrak{M} = (f_1 \ldots f_\varrho); \quad \text{d. h.} \quad f = a_1 f_1 + \ldots + a_\varrho f_\varrho + n_1 f_1 + \ldots + n_\varrho f_\varrho$$

wird für jedes $f \equiv 0\,(\mathfrak{M})$, wobei die a_i Größen des *Ringbereiches*, die n_i ganze Zahlen sind, so wird $\mathfrak{M}$ als *endliches Ideal* bezeichnet; $f_1, \ldots, f_\varrho$ als eine *Idealbasis.*

Wir legen nun im folgenden nur *solche Ringe* Σ *zugrunde, die die Endlichkeitsbedingung erfüllen: Jedes Ideal in* Σ *ist ein endliches, besitzt also eine Idealbasis.*

3. Aus der Endlichkeitsbedingung folgt direkt der allen folgenden Überlegungen zugrunde liegende

Satz I (*Satz von der endlichen Kette*)[9]): *Ist* $\mathfrak{M}, \mathfrak{M}_1, \mathfrak{M}_2, \ldots, \mathfrak{M}_\nu, \ldots$

[8]) Ideale werden mit großen deutschen Buchstaben bezeichnet. $\mathfrak{M}$ soll an das Beispiel des gewöhnlich als „Modul" oder Formenmodul bezeichneten Ideals aus Polynomen erinnern. Übrigens benutzen die §§ 1—3 nur die Modul- und nicht die Idealeigenschaft; vgl. dazu § 9.

[9]) Zuerst ausgesprochen für Zahlenmoduln von Dedekind: Zahlentheorie, Suppl. XI, § 172, Satz VIII (4. Auflage); unser Beweis und die Bezeichnung „Kette" ist von dort übernommen. Für Ideale aus Polynomen bei Lasker, a. a. O. S. 56 (Hilfssatz). Der Satz findet aber in beiden Fällen nur vereinzelte Anwendung. Unsere Anwenwendungen beruhen durchweg auf dem *Auswahlpostulat.*

ein abzählbar unendliches System von Idealen in Σ, von denen jedes durch das folgende teilbar ist, so sind von einem endlichen Index n an alle Ideale identisch, $\mathfrak{M}_n = \mathfrak{M}_{n+1} = \ldots$. M. a. W.: *Bildet* $\mathfrak{M}, \mathfrak{M}_1, \mathfrak{M}_2, \ldots, \mathfrak{M}_\nu, \ldots$ *eine einfach geordnete Kette von Idealen derart, daß jedes Ideal ein echter Teiler des unmittelbar vorangehenden ist, so bricht die Kette im Endlichen ab.*

Es sei nämlich $\mathfrak{D} = (\mathfrak{M}_1, \mathfrak{M}_2, \ldots, \mathfrak{M}_\nu, \ldots)$ der größte gemeinsame Teiler des Systems und $f_1 \ldots f_k$ eine infolge der Endlichkeitsbedingung stets existierende Basis von $\mathfrak{D}$. Dann folgt aus der Teilbarkeitsvoraussetzung, daß jedes Element von $\mathfrak{D}$ zugleich Element eines Ideals der Kette ist; denn aus

$$f = g + h, \quad g \equiv 0\,(\mathfrak{M}_r), \quad h \equiv 0\,(\mathfrak{M}_s), \quad (r \leqq s)$$

folgt $g \equiv 0\,(\mathfrak{M}_s)$ und also $f \equiv 0\,(\mathfrak{M}_s)$. Entsprechendes gilt, wenn f Summe von mehreren Bestandteilen ist. Es gibt also auch einen endlichen Index n, derart, daß

$$f_1 \equiv 0\,(\mathfrak{M}_n);\ \ldots;\ f_k \equiv 0\,(\mathfrak{M}_n);\ \mathfrak{D} = (f_1 \ldots f_k) \equiv 0\,(\mathfrak{M}_n).$$

Da umgekehrt $\mathfrak{M}_n \equiv 0\,(\mathfrak{D})$, so wird $\mathfrak{M}_n = \mathfrak{D}$; und da weiter

$$\mathfrak{M}_{n+i} \equiv 0\,(\mathfrak{D}); \quad \mathfrak{D} = \mathfrak{M}_n \equiv 0\,(\mathfrak{M}_{n+i}),$$

so wird auch $\mathfrak{M}_{n+i} = \mathfrak{D} = \mathfrak{M}_n$ für jedes i, womit der Satz bewiesen ist.

Es sei bemerkt, daß aus diesem Satz umgekehrt wieder die Existenz der Idealbasis folgt, so daß die *Endlichkeitsbedingung auch in dieser basisfreien Form* hätte ausgesprochen werden können.

§ 2.

Darstellung eines Ideals als kleinstes gemeinsames Vielfaches von endlich vielen irreduziblen Idealen.

Das *kleinste gemeinsame Vielfache* $[\mathfrak{B}_1, \mathfrak{B}_2, \ldots, \mathfrak{B}_k]$ der Ideale $\mathfrak{B}_1, \mathfrak{B}_2, \ldots, \mathfrak{B}_k$ sei wie üblich definiert als Gesamtheit der Elemente, die sowohl durch $\mathfrak{B}_1$, wie durch $\mathfrak{B}_2, \ldots$ wie durch $\mathfrak{B}_k$ teilbar sind; in Zeichen:

$$\text{aus } f \equiv 0\,(\mathfrak{B}_i),\ (i = 1, 2, \ldots, k), \text{ folgt: } f \equiv 0\,([\mathfrak{B}_1, \mathfrak{B}_2, \ldots, \mathfrak{B}_k])$$

und umgekehrt. Das kleinste gemeinsame Vielfache wird wieder ein Ideal; die Ideale $\mathfrak{B}_i$ bezeichnen wir auch als *Komponenten der Zerlegung.*

Definition I. *Eine Darstellung* $\mathfrak{M} = [\mathfrak{B}_1 \ldots \mathfrak{B}_k]$ *heißt reduzierte Darstellung, wenn kein* $\mathfrak{B}_i$ *im kleinsten gemeinsamen Vielfachen* $\mathfrak{A}_i$ *der übrigen Ideale aufgeht, und wenn kein* $\mathfrak{B}_i$ *sich durch einen echten Teiler ersetzen läßt*[10]. *Sind die Bedingungen nur für das Ideal* $\mathfrak{B}_i$ *erfüllt, so*

[10]) Ein Beispiel einer nicht reduzierten Darstellung ist:

$$(x^2, xy) = [(x), (x^2, xy, y^\lambda)]$$

heißt die Darstellung reduziert in bezug auf $\mathfrak{B}_i$. *Das kleinste gemeinsame Vielfache* $\mathfrak{A}_i = [\mathfrak{B}_1, \ldots, \mathfrak{B}_{i-1}, \mathfrak{B}_{i+1}, \ldots, \mathfrak{B}_k]$ *wird als Komplement von* $\mathfrak{B}_i$ *bezeichnet. Darstellungen, bei denen nur die erste Bedingung erfüllt ist, heißen kürzeste Darstellungen.*

Es genügt nun, sich bei der Darstellung eines Ideals als kleinstes gemeinsames Vielfaches auf reduzierte Darstellungen zu beschränken, nach

Hilfssatz I. *Jede Darstellung eines Ideals als kleinstes gemeinsames Vielfaches von endlich vielen Idealen läßt sich auf mindestens eine Art durch eine reduzierte Darstellung ersetzen; eine solche Darstellung läßt sich insbesondere erreichen durch sukzessive Zerlegung.*

Sei nämlich $\mathfrak{M} = [\mathfrak{B}_1^* \ldots \mathfrak{B}_l^*]$ eine beliebige Darstellung von $\mathfrak{M}$, so lassen wir der Reihe nach diejenigen $\mathfrak{B}_i^*$ fort, die im kleinsten gemeinsamen Vielfachen der stehen gelassenen aufgehen. Da die übrigen Ideale noch $\mathfrak{M}$ ergeben, ist in der so entstehenden Darstellung:

$$\mathfrak{M} = [\mathfrak{B}_1 \ldots \mathfrak{B}_k] = [\mathfrak{A}_i, \mathfrak{B}_i]$$

dann die erste Bedingung erfüllt, sie ist also eine kürzeste Darstellung; und diese Bedingung bleibt erfüllt, wenn man irgendein $\mathfrak{B}_i$ durch einen echten Teiler ersetzt. Die zweite Bedingung aber ist nach dem Satz von der endlichen Kette (Satz I) stets erfüllbar. Denn sei gesetzt:

$$\mathfrak{M} = [\mathfrak{A}_i, \mathfrak{B}_i] = [\mathfrak{A}_i, \mathfrak{B}_i^{(1)}] = \ldots = [\mathfrak{A}_i, \mathfrak{B}_i^{(\nu)}], \ldots,$$

wo jedes $\mathfrak{B}_i^{(\nu)}$ ein echter Teiler des unmittelbar vorangehenden ist, so muß nach diesem Satz die Kette $\mathfrak{B}_i, \mathfrak{B}_i^{(1)}, \ldots, \mathfrak{B}_i^{(\nu)}, \ldots$ im Endlichen abbrechen; in der Darstellung: $\mathfrak{M} = [\mathfrak{A}_i, \mathfrak{B}_i^{(n)}]$ läßt sich also $\mathfrak{B}_i^{(n)}$ durch keinen echten Teiler ersetzen; und dies gilt a fortiori, wenn man $\mathfrak{A}_i$ durch einen echten Teiler ersetzt. Wendet man also das Verfahren der Reihe nach auf jedes $\mathfrak{B}_i$ an, indem man jeweils das Komplement mit den schon reduzierten $\mathfrak{B}$ bildet, so entsteht eine reduzierte Darstellung[11]).

Um eine solche Darstellung sukzessiv zu gewinnen, ist zu zeigen, daß aus den einzelnen reduzierten Darstellungen:

$$\mathfrak{M} = [\mathfrak{B}_1, \mathfrak{C}_1], \quad \mathfrak{C}_1 = [\mathfrak{B}_2, \mathfrak{C}_2], \quad \ldots, \quad \mathfrak{C}_{l-1} = [\mathfrak{B}_l, \mathfrak{C}_l]$$

folgt, daß auch die daraus entstehende Darstellung: $\mathfrak{M} = [\mathfrak{B}_1 \ldots \mathfrak{B}_l \mathfrak{C}_l]$

---

für jeden Exponenten $\lambda \geqq 2$; die $\lambda = 1$ entsprechende Darstellung $[(x), (x^2, y)]$ ist eine zugehörige reduzierte. (Diese Darstellung gab mir der im Krieg gefallene K. Hentzelt als einfachstes Beispiel einer nicht eindeutigen Zerlegung in primäre Ideale an.)

[11]) Daß eine solche durch die gegebene Darstellung nicht eindeutig definiert ist, zeigt das vorige Beispiel. Für $(x^2, xy) = [(x), (x^2, xy, y^\lambda)]$, wo $\lambda \geqq 2$, ist neben $[(x), (x^2, y)]$ auch $[(x), (x^2, \mu x + y)]$ für beliebiges μ eine reduzierte Darstellung.

reduziert ist. Dazu genügt es zu zeigen, daß mit den reduzierten Darstellungen:

$$\mathfrak{M} = [\mathfrak{B}_1 \ldots \mathfrak{B}_\varrho \mathfrak{C}]; \quad \mathfrak{C} = [\mathfrak{C}_1, \mathfrak{C}_2] \quad \text{auch} \quad \mathfrak{M} = [\mathfrak{B}_1 \ldots \mathfrak{B}_\varrho \mathfrak{C}_1 \mathfrak{C}_2]$$

reduziert ist. In der Tat geht hier nach Voraussetzung kein $\mathfrak{B}$ in seinem Komplement auf; wäre dies für ein $\mathfrak{C}_i$ der Fall, so wäre gegen die Voraussetzung in der ersten Darstellung $\mathfrak{C}$ durch einen echten Teiler ersetzbar, da wegen der zweiten reduzierten Darstellung $\mathfrak{C}_1$ und $\mathfrak{C}_2$ echte Teiler von $\mathfrak{C}$ sind; die Darstellung wird also eine kürzeste. Ferner läßt sich nach Voraussetzung kein $\mathfrak{B}$ durch einen echten Teiler ersetzen; wäre dies für ein $\mathfrak{C}_i$ der Fall, so entspräche dies gegen Voraussetzung dem Ersetzen von $\mathfrak{C}$ durch einen echten Teiler, da die Darstellung für $\mathfrak{C}$ reduziert ist. Somit ist der *Hilfssatz bewiesen.*

Definition II. *Ein Ideal $\mathfrak{M}$ heißt reduzibel, wenn es als kleinstes gemeinsames Vielfaches von zwei echten Teilern darstellbar ist; im entgegengesetzten Fall heißt $\mathfrak{M}$ irreduzibel.*

Wir beweisen jetzt vermöge des Satzes I von der endlichen Kette unter Benutzung der reduzierten Darstellung

Satz II. *Jedes Ideal ist darstellbar als kleinstes gemeinsames Vielfaches von endlich vielen irreduziblen Idealen*[12]).

Es ist nämlich ein beliebiges Ideal $\mathfrak{M}$ entweder irreduzibel; dann ist $\mathfrak{M} = [\mathfrak{M}]$ eine Darstellung, wie Satz II verlangt; oder aber es wird $\mathfrak{M} = [\mathfrak{B}_1, \mathfrak{C}_1]$, wo $\mathfrak{B}_1, \mathfrak{C}_1$ echte Teiler von $\mathfrak{M}$ sind, und wo die Darstellung nach Hilfssatz I als reduziert angenommen werden kann. Für $\mathfrak{C}_1$ gilt die gleiche Alternative; entweder es ist irreduzibel oder es gibt eine reduzierte Darstellung: $\mathfrak{C}_1 = [\mathfrak{B}_2, \mathfrak{C}_2]$.

So fortfahrend erhält man die Reihe reduzierter Darstellungen:

$$(1) \qquad \mathfrak{M} = [\mathfrak{B}_1, \mathfrak{C}_1]; \; \mathfrak{C}_1 = [\mathfrak{B}_2, \mathfrak{C}_2]; \; \ldots, \mathfrak{C}_{\nu-1} = [\mathfrak{B}_\nu, \mathfrak{C}_\nu]; \; \ldots.$$

In der Kette $\mathfrak{C}_1, \mathfrak{C}_2, \ldots, \mathfrak{C}_\nu, \ldots$ ist also jeweils $\mathfrak{C}_i$ ein echter Teiler des unmittelbar vorangehenden, und folglich bricht die Kette im Endlichen ab; es gibt einen Index n, so daß $\mathfrak{C}_n$ irreduzibel wird. Nach Hilfssatz I ist ferner die Darstellung: $\mathfrak{M} = [\mathfrak{B}_1 \ldots \mathfrak{B}_n \mathfrak{C}_n]$ reduziert; $\mathfrak{C}_n$ kann also nicht in seinem Komplement $\mathfrak{A}_n$ aufgehen, und in der Darstellung: $\mathfrak{M} = [\mathfrak{A}_n, \mathfrak{C}_n]$ ist $\mathfrak{C}_n$ durch keinen echten Teiler ersetzbar. Ersetzt man

[12]) Daß eine solche Darstellung im allgemeinen nicht eindeutig ist, zeigt das vorige Beispiel: $(x^2, xy) = [(x), (x^2, \mu x + y)]$. Die beiden Komponenten sind bei beliebigem μ irreduzibel. Alle Teiler von (x) sind nämlich von der Form $(x, g(y))$, wo $g(y)$ ein Polynom in y bedeutet; also hat auch das kleinste gemeinsame Vielfache von zweien diese Form, wird also ein echter Teiler von (x); $(x^2, \mu x + y)$ besitzt nur den *einen* Teiler (x, y), ist also notwendigerweise ebenfalls irreduzibel.

nötigenfalls $\mathfrak{A}_n$ durch einen echten Teiler[13]), so daß die Darstellung reduziert wird, so ist damit gezeigt, daß jedes *reduzible Ideal eine reduzierte Darstellung als kleinstes gemeinsames Vielfaches eines irreduziblen und eines dazu komplementären Ideals zuläßt.* In der Reihe (1) können also ohne Beschränkung der Allgemeinheit alle $\mathfrak{B}_i$ als irreduzibel angenommen werden; die Wiederholung der obigen Schlußweise ergibt die Existenz eines irreduziblen $\mathfrak{C}_n$, womit *Satz* II *bewiesen ist.*

§ 3.

Anzahlgleichheit der Komponenten bei zwei verschiedenen Zerlegungen in irreduzible Ideale.

Zum Beweise der Anzahlgleichheit ist vorerst die Reduzibilität bzw. Irreduzibilität eines Ideals durch Eigenschaften seines Komplementes auszudrücken nach

Satz III[14]). *Die kürzeste Darstellung* $\mathfrak{M} = [\mathfrak{A}, \mathfrak{C}]$ *sei reduziert in bezug auf* $\mathfrak{C}$. *Dann ist die notwendige und hinreichende Bedingung dafür, daß* $\mathfrak{C}$ *reduzibel ist, die Existenz von zwei Idealen* $\mathfrak{N}_1$ *und* $\mathfrak{N}_2$, *die echte Teiler von* $\mathfrak{M}$ *sind, derart, daß*

$$(2) \qquad \mathfrak{N}_1 \equiv 0\,(\mathfrak{A}); \quad \mathfrak{N}_2 \equiv 0\,(\mathfrak{A}); \quad [\mathfrak{N}_1, \mathfrak{N}_2] = \mathfrak{M}.$$

Hieraus folgt noch: *Sind die Bedingungen* (2) *erfüllt, und* $\mathfrak{C}$ *irreduzibel, so ist mindestens ein* $\mathfrak{N}_i$ *kein echter Teiler von* $\mathfrak{M}$; $\mathfrak{N}_i = \mathfrak{M}$.

Es sei $\mathfrak{C} = [\mathfrak{C}_1, \mathfrak{C}_2]$, wo $\mathfrak{C}_1, \mathfrak{C}_2$ echte Teiler von $\mathfrak{C}$ seien. Dann kommt:

$$\mathfrak{M} = [\mathfrak{A}, \mathfrak{C}] = [\mathfrak{A}, \mathfrak{C}_1, \mathfrak{C}_2] = [[\mathfrak{A}, \mathfrak{C}_1], [\mathfrak{A}, \mathfrak{C}_2]].$$

Hier sind die Ideale $[\mathfrak{A}, \mathfrak{C}_i]$ echte Teiler von $\mathfrak{M}$, da sonst $[\mathfrak{A}, \mathfrak{C}]$ nicht reduziert in bezug auf $\mathfrak{C}$ wäre. Da auch die Teilbarkeit durch $\mathfrak{A}$ erfüllt ist, ist die *Bedingung* (2) *als notwendig erwiesen.* (Die Darstellung (2) ist nicht reduziert, da ein $[\mathfrak{A}, \mathfrak{C}_i]$ durch $\mathfrak{C}_i$ ersetzbar ist.)

Sei nun umgekehrt (2) erfüllt. Wir bilden die Ideale:

$$\mathfrak{C}_1 = (\mathfrak{C}, \mathfrak{N}_1); \quad \mathfrak{C}_2 = (\mathfrak{C}, \mathfrak{N}_2); \quad \mathfrak{C}^* = [\mathfrak{C}_1, \mathfrak{C}_2].$$

Dann ist $\mathfrak{C}$ sowohl durch $\mathfrak{C}_1$, wie durch $\mathfrak{C}_2$, also auch durch das kleinste gemeinsame Vielfache $\mathfrak{C}^*$ teilbar. Um die Teilbarkeit von $\mathfrak{C}^*$ durch $\mathfrak{C}$ zu zeigen, sei

---

[13]) Tatsächlich ist die Darstellung auch in bezug auf $\mathfrak{A}_n$ reduziert, wie in § 3 (Hilfssatz IV) als Umkehrung von Hilfssatz I gezeigt werden wird.

[14]) Satz III entspricht dem Übergang von den Moduln zu den Restgruppen in den Arbeiten von Schmeidler und Noether-Schmeidler (vgl. die Einleitung). Es entspricht $\mathfrak{A}$ der Restgruppe, $\mathfrak{N}_1$ und $\mathfrak{N}_2$ den Untergruppen, in welche die Restgruppe zerlegt wird.

$f \equiv 0\,(\mathfrak{C}^*)$; also $f \equiv 0\,(\mathfrak{C}_1)$; $f \equiv 0\,(\mathfrak{C}_2)$ oder auch $f = c + n_1$; $f = \bar{c} + n_2$, wo c, $\bar{c}$, n_1, n_2 Größen aus $\mathfrak{C}$, $\mathfrak{N}_1$, $\mathfrak{N}_2$ sind, also insbesondere n_i durch $\mathfrak{A}$ teilbar ist. Somit ist die Differenz

$$g = c - \bar{c} = n_2 - n_1$$

sowohl durch $\mathfrak{C}$ wie durch $\mathfrak{A}$, also durch $\mathfrak{M}$ teilbar. Wegen $n_1 = n_2 + m$ ist ferner n_1 (ebenso n_2) sowohl durch $\mathfrak{N}_1$ wie durch $\mathfrak{N}_2$, also durch $\mathfrak{M}$ teilbar. Also wird

$$f = c + m; \quad f \equiv 0\,(\mathfrak{C}); \quad \mathfrak{C}^* = \mathfrak{C}.$$

$\mathfrak{C}_1$ und $\mathfrak{C}_2$ sind dabei echte Teiler von $\mathfrak{C}$; denn für $\mathfrak{C}_i = (\mathfrak{C}, \mathfrak{N}_i) = \mathfrak{C}$ wäre $\mathfrak{N}_i$ durch $\mathfrak{C}$ teilbar, also wäre $\mathfrak{N}_i$ wegen der Teilbarkeit durch $\mathfrak{A}$ gleich $\mathfrak{M}$ gegen die Voraussetzung. Somit ist $\mathfrak{C} = [\mathfrak{C}_1, \mathfrak{C}_2]$ als reduzibel erkannt; *Satz* III *bewiesen.*

Es sei bemerkt, daß fast die gleiche Überlegung noch das folgende zeigt:

Hilfssatz II. *Läßt sich in einer kürzesten Darstellung* $\mathfrak{M} = [\mathfrak{A}, \mathfrak{C}]$, *das Ideal* $\mathfrak{C}$ *durch einen echten Teiler ersetzen, so ist* $\mathfrak{C}$ *reduzibel.*

Sei also:

$$\mathfrak{M} = [\mathfrak{A}, \mathfrak{C}] = [\mathfrak{A}, \mathfrak{C}_1],$$

und sei gesetzt:

$$\mathfrak{C}^* = [\mathfrak{C}_1, (\mathfrak{A}, \mathfrak{C})],$$

dann ist wieder $\mathfrak{C}$ durch $\mathfrak{C}^*$ teilbar. Aus $f \equiv 0\,(\mathfrak{C}^*)$ folgt ferner:

$$f = c_1 = a + c.$$

Die Differenz $a = c_1 - c$ ist also sowohl durch $\mathfrak{A}$, wie durch $\mathfrak{C}_1$, folglich durch $\mathfrak{M}$ teilbar; also wird $c_1 = c + m$; $f \equiv 0\,(\mathfrak{C})$; $\mathfrak{C}^* = \mathfrak{C}$.

Da sowohl $\mathfrak{C}_1$ wie $(\mathfrak{A}, \mathfrak{C})$ nach Voraussetzung echte Teiler von $\mathfrak{C}$ sind, ist somit $\mathfrak{C} = \mathfrak{C}^*$ als reduzibel erkannt.

Ein *irreduzibles* $\mathfrak{C}$ läßt sich also nicht durch einen echten Teiler ersetzen.

Es seien jetzt *zwei verschiedene kürzeste Darstellungen von* $\mathfrak{M}$ *als kleinstes gemeinsames Vielfaches von (endlich) vielen irreduziblen Idealen gegeben*:

$$\mathfrak{M} = [\mathfrak{B}_1 \ldots \mathfrak{B}_k] = [\mathfrak{D}_1 \ldots \mathfrak{D}_l].$$

Diese Darstellungen sind nach der Bemerkung zu Hilfssatz II zugleich *reduziert.* Dann beweisen wir vorerst

Hilfssatz III. *Zu jedem Komplement* $\mathfrak{A}_i = [\mathfrak{B}_1 \ldots \mathfrak{B}_{i-1}\, \mathfrak{B}_{i+1} \ldots \mathfrak{B}_k]$ *gibt es ein Ideal* $\mathfrak{D}_j$ *derart, daß* $\mathfrak{M} = [\mathfrak{A}_i, \mathfrak{D}_j]$ *wird.*

Setzt man nämlich: $\mathfrak{M} = [\mathfrak{D}_1, \mathfrak{C}_1]$, $\mathfrak{C}_1 = [\mathfrak{D}_2, \mathfrak{C}_{12}]$ usf., so kommt:

$$\mathfrak{M} = [\mathfrak{A}_i, \mathfrak{M}] = [\mathfrak{A}_i, \mathfrak{D}_1, \mathfrak{C}_1] = [[\mathfrak{A}_i \mathfrak{D}_1], [\mathfrak{A}_i \mathfrak{C}_1]].$$

Hier sind für $\mathfrak{N}_1 = [\mathfrak{A}_i, \mathfrak{D}_1]$, $\mathfrak{N}_2 = [\mathfrak{A}_i, \mathfrak{C}_1]$ die Bedingungen (2) von Satz III erfüllt, da $\mathfrak{M} = [\mathfrak{A}_i, \mathfrak{B}_i]$ reduziert in bezug auf $\mathfrak{B}_i$ ist und die Darstellung eine kürzeste ist. Da nun $\mathfrak{B}_i$ als *irreduzibel* vorausgesetzt war, muß notwendig ein $\mathfrak{N}_i$ gleich $\mathfrak{M}$ werden.

Für $\mathfrak{N}_1 = \mathfrak{M}$ wäre der Hilfssatz bewiesen; für $\mathfrak{N}_2 = \mathfrak{M}$ kommt entsprechend: $\mathfrak{M} = [[\mathfrak{A}_i \mathfrak{D}_2], [\mathfrak{A}_i \mathfrak{C}_{12}]]$, wo nach dem gleichen Schluß wieder eine Komponente gleich $\mathfrak{M}$ werden muß. So fortfahrend, kommt entweder: $\mathfrak{M} = [\mathfrak{A}_i, \mathfrak{D}_j]$, wo $j < l$; oder es wird $\mathfrak{M} = [\mathfrak{A}_i, \mathfrak{C}_{1 \dots l-1}]$; wegen $\mathfrak{C}_{1 \dots l-1} = \mathfrak{D}_l$ ist damit der *Hilfssatz bewiesen.*

Hieraus ergibt sich nun

Satz IV. *Bei zwei verschiedenen kürzesten Darstellungen eines Ideals als kleinstes gemeinsames Vielfaches von irreduziblen ist die Anzahl der Komponenten die gleiche.*

Aus dem Hilfssatz ergibt sich nämlich für $i = 1$:

$$\mathfrak{M} = [\mathfrak{A}_1, \mathfrak{B}_1] = [\mathfrak{A}_1, \mathfrak{D}_{j_1}] = [\mathfrak{D}_{j_1}, \mathfrak{B}_2, \dots, \mathfrak{B}_k].$$

Betrachtet man nun die beiden Zerlegungen:

$$\mathfrak{M} = [\mathfrak{D}_{j_1}, \mathfrak{B}_2, \dots, \mathfrak{B}_k] = [\mathfrak{D}_1, \mathfrak{D}_2, \dots, \mathfrak{D}_l],$$

und wiederholt den obigen Schluß in bezug auf das Komplement $\overline{\mathfrak{A}}_2 = [\mathfrak{D}_{j_1}, \mathfrak{B}_3, \dots, \mathfrak{B}_k]$ von $\mathfrak{B}_2$, so kommt:

$$\mathfrak{M} = [\overline{\mathfrak{A}}_2, \mathfrak{B}_2] = [\overline{\mathfrak{A}}_2, \mathfrak{D}_{j_2}] = [\mathfrak{D}_{j_1}, \mathfrak{D}_{j_2} \mathfrak{B}_3, \dots, \mathfrak{B}_k];$$

und durch Fortsetzung des Verfahrens:

$$\mathfrak{M} = [\mathfrak{D}_{j_1}, \mathfrak{D}_{j_2}, \dots, \mathfrak{D}_{j_k}].$$

Da nun nach Voraussetzung die Darstellung $\mathfrak{M} = [\mathfrak{D}_1 \dots \mathfrak{D}_l]$ eine kürzeste ist, also kein $\mathfrak{D}$ weggelassen werden kann, müssen die *verschiedenen* unter den $\mathfrak{D}_{j_i}$ alle $\mathfrak{D}$ erschöpfen; somit kommt: $k \geqq l$. Vertauscht man im Hilfssatz und den anschließenden Schlüssen durchweg die $\mathfrak{B}$ mit den $\mathfrak{D}$, so kommt entsprechend: $l \geqq k$, und somit $k = l$, womit die *Anzahlgleichheit* bewiesen ist. — Daraus ergibt sich noch, daß die Ideale $\mathfrak{D}_{j_i}$ alle untereinander verschieden sind, da sonst in einer kürzesten Darstellung durch die $\mathfrak{D}_{j_i}$ weniger als k Komponenten auftreten würden; man kann also die Bezeichnung so wählen, daß $\mathfrak{D}_{j_i} = \mathfrak{D}_i$ wird. Aus dem gleichen Grunde sind auch alle Zwischendarstellungen $\mathfrak{M} = [\mathfrak{D}_{j_1} \dots \mathfrak{D}_{j_i}, \mathfrak{B}_{i+1} \dots \mathfrak{B}_k]$ kürzeste und nach der Bemerkung zu Hilfssatz II somit reduzierte.

Die Anzahlgleichheit führt zu einer Umkehrung von Hilfssatz I durch

Hilfssatz IV. *Faßt man in einer reduzierten Darstellung die Komponenten zu Gruppen zusammen und bildet deren kleinstes gemeinsames Vielfaches, so wird die entstehende Darstellung reduziert.* M. a. W.: *Aus einer reduzierten Darstellung*

$$\mathfrak{M} = [\mathfrak{C}_{11} \dots \mathfrak{C}_{1\mu_1}; \dots; \mathfrak{C}_{\sigma 1} \dots \mathfrak{C}_{\sigma\mu_\sigma}]$$

folgt, daß auch $\mathfrak{M} = [\mathfrak{N}_1 \dots \mathfrak{N}_\sigma] = [\mathfrak{N}_i, \mathfrak{L}_i]$ *reduziert ist, wenn* $\mathfrak{N}_i = [\mathfrak{C}_{i1} \dots \mathfrak{C}_{i\mu_i}]$ *gesetzt ist.*

Zuerst ist zu bemerken, daß $\mathfrak{N}_i$ nicht in seinem Komplement $\mathfrak{L}_i$ aufgehen kann, da dies für keinen seiner Teiler $\mathfrak{C}_{ij}$ der Fall ist; die Darstellung ist also eine kürzeste. Um zu zeigen, daß $\mathfrak{N}_i$ durch keinen echten Teiler ersetzbar ist, lösen wir die $\mathfrak{C}$ in ihre irreduziblen Ideale $\mathfrak{B}$ auf[15]), so daß die (nach Hilfssatz I) reduzierten Darstellungen enstehen:

$$\mathfrak{M} = [\mathfrak{B}_{11} \dots \mathfrak{B}_{1\lambda_1}; \dots; \mathfrak{B}_{\sigma 1} \dots \mathfrak{B}_{\sigma\lambda_\sigma}]; \qquad \mathfrak{N}_i = [\mathfrak{B}_{i1} \dots \mathfrak{B}_{i\lambda_i}].$$

Es sei nun $\mathfrak{M} = [\mathfrak{N}_i^*, \mathfrak{L}_i]$ reduziert in bezug auf $\mathfrak{N}_i^*$, und $\mathfrak{N}_i^*$ ein *echter* Teiler von $\mathfrak{N}_i$. Nach Hilfssatz II wird:

$$\mathfrak{N}_i = [\mathfrak{N}_i^*, (\mathfrak{N}_i, \mathfrak{L}_i)];$$

und diese Darstellung ist notwendig reduziert in bezug auf $\mathfrak{N}_i^*$, da sich sonst $\mathfrak{N}_i^*$ auch in $\mathfrak{M}$ durch einen echten Teiler ersetzen ließe. Man ersetze nun gegebenenfalls auch $(\mathfrak{N}_i, \mathfrak{L}_i)$ durch einen echten Teiler, so daß eine reduzierte Darstellung für $\mathfrak{N}_i$ entsteht. Löst man jetzt die beiden Komponenten von $\mathfrak{N}_i$ in irreduzible Ideale auf, so setzt sich die Anzahl λ_i der irreduziblen Ideale von $\mathfrak{N}_i$ additiv aus der der Komponenten zusammen; die Anzahl der dem echten Teiler $\mathfrak{N}_i^*$ entsprechenden irreduziblen Ideale wird also notwendig kleiner als λ_i. Dann führt aber auch die Auflösung von $\mathfrak{M} = [\mathfrak{N}_i^*, \mathfrak{L}]$ in irreduzible Ideale zu weniger als $\sum_i \lambda_i$ Ideale, im *Widerspruch mit der Anzahlgleichheit.* Als Spezialfall $\sigma = 2$ folgt noch, daß die Darstellung $\mathfrak{M} = [\mathfrak{N}_i, \mathfrak{L}_i]$ auch in bezug auf das Komplement $\mathfrak{L}_i$ reduziert ist.

§ 4.

Primäre Ideale. Eindeutigkeit der zugehörigen Primideale bei zwei verschiedenen Zerlegungen in irreduzible Ideale.

Es handelt sich im folgenden um den Zusammenhang zwischen primären und irreduziblen Idealen.

Definition III. *Ein Ideal* $\mathfrak{Q}$ *heißt primär, wenn aus* $a \cdot b \equiv 0\,(\mathfrak{Q})$; $a \not\equiv 0\,(\mathfrak{Q})$ *notwendig folgt:* $b^\varkappa \equiv 0\,(\mathfrak{Q})$, *wo der Exponent* $\varkappa$ *eine endliche Zahl ist.*

Die Definition läßt sich auch so aussprechen: Ist ein Produkt $a \cdot b$ durch $\mathfrak{Q}$ teilbar, so ist entweder ein Faktor teilbar oder eine Potenz jedes Faktors. *Ist insbesondere* $\varkappa$ *stets gleich* 1, *so heißt das Ideal ein Primideal.*

[15]) Darunter ist immer eine kürzeste, also reduzierte Darstellung durch die $\mathfrak{B}$ zu verstehen.

Aus der Definition des primären (bzw. Prim-) Ideals folgt vermöge der Basisexistenz die nur von Produkten von Idealen[16]) handelnde

Definition III a. *Ein Ideal* $\mathfrak{Q}$ *heißt primär, wenn aus* $\mathfrak{A}\cdot\mathfrak{B}\equiv 0\,(\mathfrak{Q})$; $\mathfrak{A}\not\equiv 0\,(\mathfrak{Q})$ *notwendig folgt:* $\mathfrak{B}^{\lambda}\equiv 0\,(\mathfrak{Q})$. *Ist* λ *stets gleich* 1, *so heißt das Ideal ein Primideal. Für ein Primideal* $\mathfrak{P}$ *folgt also aus* $\mathfrak{A}\cdot\mathfrak{B}\equiv 0\,(\mathfrak{P})$, $\mathfrak{A}\not\equiv 0\,(\mathfrak{P})$ *stets* $\mathfrak{B}\equiv 0\,(\mathfrak{P})$.

Da nämlich in III a für $\mathfrak{A}=(a)$, $\mathfrak{B}=(b)$ die Definition III als Spezialfall enthalten ist, ist jedes nach III a primäre Ideal auch primär nach III. Sei umgekehrt $\mathfrak{Q}$ primär nach III, und sei die Voraussetzung von III a erfüllt: $\mathfrak{A}\cdot\mathfrak{B}\equiv 0\,(\mathfrak{Q})$, so daß also entweder $\mathfrak{A}\equiv 0\,(\mathfrak{Q})$ folgt, oder aber daß es mindestens eine Größe $a\equiv 0\,(\mathfrak{A})$ gibt, so daß $a\cdot\mathfrak{B}\equiv 0\,(\mathfrak{Q})$, $a\not\equiv 0\,(\mathfrak{Q})$ wird. Ist nun $b_1\ldots b_r$ eine Idealbasis von $\mathfrak{B}$, so kommt nach Definition III, da $a\cdot b_i\equiv 0\,(\mathfrak{Q})$ wird:

$$b_1^{\varkappa_1}\equiv 0\,(\mathfrak{Q});\ \ldots;\ b_r^{\varkappa_r}\equiv 0\,(\mathfrak{Q}).$$

Wegen $b=f_1b_1+\ldots+f_rb_r+n_1b_1+\ldots+n_rb_r$ wird also für $\lambda=\varkappa_1+\ldots+\varkappa_r$ das Produkt von je λ Größen b durch $\mathfrak{Q}$ teilbar, womit für nach III primäre Ideale das Erfülltsein der Definition III a bewiesen ist. Speziell für Primideale $\mathfrak{P}$ folgt aber aus: $a\cdot\mathfrak{B}\equiv 0\,(\mathfrak{P})$, also auch $a\cdot b\equiv 0\,(\mathfrak{P})$ für jedes $b\equiv 0\,(\mathfrak{B})$ und $a\not\equiv 0\,(\mathfrak{P})$, daß $b\equiv 0\,(\mathfrak{P})$ und damit $\mathfrak{B}\equiv 0\,(\mathfrak{P})$. Damit ist die Äquivalenz der beiden Definitionen gezeigt.

Der Zusammenhang zwischen primären und Prim-Idealen wird hergestellt durch die Bemerkung, daß die Gesamtheit $\mathfrak{P}$ aller Elemente p von der Eigenschaft, daß eine Potenz von p durch $\mathfrak{Q}$ teilbar ist, ein *Primideal* bildet. Zunächst ist klar, daß $\mathfrak{P}$ ein Ideal ist; da neben p_1 und p_2 auch ap_1 und (p_1-p_2) die genannte Eigenschaft zukommt. Nach dem bei der Definition von III a angewandten Basisschluß ergibt sich ferner die Existenz einer Zahl λ, derart, daß $\mathfrak{P}^{\lambda}\equiv 0\,(\mathfrak{Q})$ wird.

Sei jetzt:

$$a\cdot b\equiv 0\,(\mathfrak{P});\qquad a\not\equiv 0\,(\mathfrak{P}),$$

so kommt nach der Definition von $\mathfrak{P}$:

$$a^{\lambda}\cdot b^{\lambda}\equiv 0\,(\mathfrak{Q});\qquad a^{\lambda}\not\equiv 0\,(\mathfrak{Q});$$

also nach der Definition von $\mathfrak{Q}$:

$$b^{\lambda\varkappa}\equiv 0\,(\mathfrak{Q})\quad\text{und folglich}\quad b\equiv 0\,(\mathfrak{P}),$$

womit $\mathfrak{P}$ *als Primideal nachgewiesen ist.* $\mathfrak{P}$ ist auch definiert als größter gemeinsamer Teiler aller Ideale $\mathfrak{B}$ von der Eigenschaft, daß eine Potenz von $\mathfrak{B}$ durch $\mathfrak{Q}$ teilbar ist. Denn jedes solche $\mathfrak{B}$ ist nach Definition

[16]) Unter dem Produkte $\mathfrak{A}\cdot\mathfrak{B}$ zweier Ideale wird, wie üblich, das aus der Gesamtheit der Größen $a\cdot b$ und ihren endlichen Summen bestehende Ideal verstanden.

durch $\mathfrak{P}$ teilbar; also auch der größte gemeinsame Teiler $\mathfrak{D}$ dieser $\mathfrak{B}$. Umgekehrt ist $\mathfrak{P}$ selbst ein Ideal $\mathfrak{B}$, also durch $\mathfrak{D}$ teilbar, womit $\mathfrak{P} = \mathfrak{D}$ erwiesen ist. $\mathfrak{P}$ ist also ein Primideal, das Teiler von $\mathfrak{Q}$ ist und von dem eine Potenz durch $\mathfrak{Q}$ teilbar ist; durch diese Eigenschaft ist es eindeutig definiert. Denn aus:

$$\mathfrak{Q} \equiv 0\,(\mathfrak{P}); \quad \mathfrak{P}^{\lambda} \equiv 0\,(\mathfrak{Q}); \quad \mathfrak{Q} \equiv 0\,(\overline{\mathfrak{P}}); \quad \overline{\mathfrak{P}}^{\mu} \equiv 0\,(\mathfrak{Q})$$

folgt:

$$\mathfrak{P}^{\lambda} \equiv 0\,(\overline{\mathfrak{P}}); \quad \overline{\mathfrak{P}}^{\mu} \equiv 0\,(\mathfrak{P});$$

also nach der Eigenschaft der Primideale:

$$\mathfrak{P} \equiv 0\,(\overline{\mathfrak{P}}); \quad \overline{\mathfrak{P}} \equiv 0\,(\mathfrak{P}); \quad \mathfrak{P} = \overline{\mathfrak{P}}.$$

Zusammenfassend haben wir

Satz V. *Zu jedem primären Ideal $\mathfrak{Q}$ existiert ein und nur ein Primideal $\mathfrak{P}$, das Teiler von $\mathfrak{Q}$ ist und von dem eine Potenz durch $\mathfrak{Q}$ teilbar ist; $\mathfrak{P}$ soll als „zugehöriges Primideal" bezeichnet werden*[17]. *$\mathfrak{P}$ ist definiert als größter gemeinsamer Teiler aller Ideale $\mathfrak{B}$ von der Eigenschaft, daß eine Potenz von $\mathfrak{B}$ durch $\mathfrak{Q}$ teilbar ist. Ist ϱ die kleinste Zahl derart, daß $\mathfrak{P}^{\varrho} \equiv 0\,(\mathfrak{Q})$, so soll ϱ als Exponent von $\mathfrak{Q}$ bezeichnet werden*[18].

Wir beweisen jetzt, als Zusammenhang zwischen primär und irreduzibel:

Satz VI. *Jedes nichtprimäre Ideal ist reduzibel; m. a. W.: jedes irreduzible Ideal ist primär*[19].

Es sei $\mathfrak{R}$ ein *nichtprimäres* Ideal, so daß nach Definition III mindestens ein Größenpaar a, b existiert, derart, daß

$$(3) \qquad a \cdot b \equiv 0\,(\mathfrak{R}); \quad a \not\equiv 0\,(\mathfrak{R}); \quad b^{\varkappa} \not\equiv 0\,(\mathfrak{R}) \quad \text{für jedes } \varkappa.$$

---

[17]) Daß die Umkehrung nicht gilt, zeigt das Beispiel $\mathfrak{M} = (x^2, xy)$. Das Primideal (x) erfüllt alle Bedingungen, aber $\mathfrak{M}$ ist nicht primär.

[18]) Daß im allgemeinen nicht, wie im Bereich der ganzen rationalen, bzw. algebraischen Zahlen, $\mathfrak{P}^{\varrho} = \mathfrak{Q}$ wird, zeigt das Beispiel:

$$\mathfrak{Q} = (x^2, y); \quad \mathfrak{P} = (x, y); \quad \mathfrak{P}^2 = (x^2, xy, y^2) \equiv 0\,(\mathfrak{Q}); \quad \text{aber } \mathfrak{Q} \not\equiv 0\,(\mathfrak{P}^2);$$

also $\mathfrak{Q}$ von $\mathfrak{P}^2$ verschieden.

[19]) Daß hier die Umkehrung nicht gilt, zeigt etwa das Beispiel:

$$\mathfrak{Q} = (x^2, xy, y^{\lambda}) = [(x^2, y), (x, y^{\lambda})],$$

wo $\lambda \geq 2$. Hier ist $\mathfrak{Q}$ primär, aber reduzibel. (Daß $\mathfrak{Q}$ primär ist, folgt daraus, daß es alle Potenzprodukte λ-ter Dimension von x, y enthält; für jedes Polynom ohne konstantes Glied ist also eine Potenz durch $\mathfrak{Q}$ teilbar. Enthält aber in $a \cdot b \equiv 0\,(\mathfrak{Q})$ das Polynom b ein konstantes Glied — also $b^{\varkappa} \not\equiv 0\,(\mathfrak{Q})$ für jedes $\varkappa$ —, so muß, da wegen der Homogenität der Basispolynome von $\mathfrak{Q}$ jeder homogene Bestandteil von $a \cdot b$ durch $\mathfrak{Q}$ teilbar ist, a durch $\mathfrak{Q}$ teilbar sein.)

Wir bilden nun die beiden Ideale:

$$\mathfrak{L}_0 = (\mathfrak{K}, a); \quad \mathfrak{N}_0 = (\mathfrak{K}, b),$$

die nach (3) echte Teiler von $\mathfrak{K}$ sind und für die nach (3) gilt:

$$\mathfrak{L}_0 \cdot \mathfrak{N}_0 \equiv 0\,(\mathfrak{K}). \tag{4}$$

Für die Elemente f des kleinsten gemeinsamen Vielfachen $\mathfrak{K}_0 = [\mathfrak{L}_0, \mathfrak{N}_0]$ gilt nun die Alternative:

Entweder es folgt aus

$$f \equiv 0\,(\mathfrak{L}_0); \quad f \equiv 0\,(\mathfrak{N}_0), \quad \text{d. h.} \quad f \equiv a_1 \cdot b\,(\mathfrak{K})$$

stets eine Darstellung:

$$f \equiv l_0 \cdot b\,(\mathfrak{K}); \quad l_0 \equiv 0\,(\mathfrak{L}_0);$$

also nach (4): $f \equiv 0\,(\mathfrak{K})$, somit $\mathfrak{K}_0 \equiv 0\,(\mathfrak{K})$, und wegen $\mathfrak{K} \equiv 0\,(\mathfrak{K}_0)$ auch $\mathfrak{K} = \mathfrak{K}_0$, womit $\mathfrak{K}$ als *reduzibel* nachgewiesen ist.

Oder es gibt mindestens ein $f \equiv 0\,(\mathfrak{K}_0)$, für das kein solches l_0 existiert. Wir bilden dann mit dem zu diesem f gehörigen a_1:

$$\mathfrak{L}_1 = (\mathfrak{L}_0, a_1) = (\mathfrak{K}, a, a_1); \quad \mathfrak{N}_1 = (\mathfrak{K}, b^2).$$

Dann wird wegen $a_1 \cdot b \equiv 0\,(\mathfrak{L}_0)$ nach (4) auch:

$$\mathfrak{L}_1 \cdot \mathfrak{N}_1 \equiv 0\,(\mathfrak{K}); \tag{4'}$$

und $\mathfrak{L}_1$ wird ein *echter* Teiler von $\mathfrak{L}_0$.

Für die Elemente f von $\mathfrak{K}_1 = [\mathfrak{L}_1, \mathfrak{N}_1]$ gilt die gleiche Alternative:

Entweder es folgt aus

$$f \equiv 0\,(\mathfrak{L}_1); \quad f \equiv 0\,(\mathfrak{N}_1);$$

d. h.: $f \equiv a_2 \cdot b^2\,(\mathfrak{K})$ stets:

$$f \equiv l_1 \cdot b^2; \quad l_1 \equiv 0\,(\mathfrak{L}_1);$$

und damit nach (4'):

$$\mathfrak{K} = \mathfrak{K}_1.$$

Oder für mindestens ein f gibt es kein solches l_1, was zur Bildung von $\mathfrak{L}_2 = (\mathfrak{L}_1, a_2)$, $\mathfrak{N}_2 = (\mathfrak{K}, b^{2^2})$ führt; mit $\mathfrak{L}_2 \cdot \mathfrak{N}_2 \equiv 0\,(\mathfrak{K})$, wo $\mathfrak{L}_2$ ein *echter* Teiler von $\mathfrak{L}_1$ ist. — So fortfahrend, definieren wir allgemein:

$$\mathfrak{L}_0 = (\mathfrak{K}, a); \ \mathfrak{L}_1 = (\mathfrak{L}_0, a_1); \ \ldots; \ \mathfrak{L}_\nu = (\mathfrak{L}_{\nu-1}, a_\nu); \ \ldots;$$

$$\mathfrak{N}_0 = (\mathfrak{K}, b); \ \mathfrak{N}_1 = (\mathfrak{K}, b^2); \ \ldots; \ \mathfrak{N}_\nu = (\mathfrak{K}, b^{2^\nu}); \ \ldots,$$

wo die a_i dadurch definiert sind, daß es ein f gibt, derart, daß

$$f \equiv 0\,(\mathfrak{L}_{i-1}); \qquad f \equiv 0\,(\mathfrak{N}_{i-1}),$$

d. h.

$$f \equiv a_i \cdot b^{2^{i-1}}\,(\mathfrak{K}); \quad \text{aber} \quad a_i \not\equiv 0\,(\mathfrak{L}_{i-1})$$

wird. Danach wird allgemein $\mathfrak{L}_i \cdot \mathfrak{N}_i \equiv 0\,(\mathfrak{K})$, $\mathfrak{N}_i$ nach (3) ein *echter* Teiler

von $\mathfrak{K}$, und $\mathfrak{L}_i$ ein *echter* Teiler von $\mathfrak{L}_{i-1}$. Nach Satz I von der endlichen Kette muß also die *Kette der* $\mathfrak{L}$ *im Endlichen, etwa mit* $\mathfrak{L}_n$, *abbrechen.* Für jedes $f \equiv 0\,(\mathfrak{L}_n)$; $f \equiv 0\,(\mathfrak{N}_n)$ wird also $f \equiv l_n \cdot b^{2^n}\,(\mathfrak{K})$ mit $l_n \equiv 0\,(\mathfrak{L}_n)$, und folglich kommt nach dem obigen Schluß: $\mathfrak{K} = [\mathfrak{L}_n, \mathfrak{N}_n]$, *womit* $\mathfrak{K}$ *als reduzibel nachgewiesen ist.*

Aus dem eben Bewiesenen ergibt sich die *Eindeutigkeit der zugehörigen Primideale* wie folgt:

Es seien

$$\mathfrak{M} = [\mathfrak{B}_1 \ldots \mathfrak{B}_k] = [\mathfrak{D}_1 \ldots \mathfrak{D}_k]$$

zwei kürzeste, also reduzierte Darstellungen von $\mathfrak{M}$ als kleinstes gemeinsames Vielfaches von irreduziblen Idealen, deren Anzahl nach Satz IV übereinstimmt. Dann sind nach diesem Satz auch die dort auftretenden Zwischendarstellungen (wo, wie dort bemerkt, der Index $j_i = i$ gesetzt werden kann):

$$\begin{aligned}\mathfrak{M} &= [\mathfrak{D}_1 \ldots \mathfrak{D}_{i-1} \mathfrak{B}_i \mathfrak{B}_{i+1} \ldots \mathfrak{B}_k] = [\mathfrak{D}_1 \ldots \mathfrak{D}_{i-1} \mathfrak{D}_i \mathfrak{B}_{i+1} \ldots \mathfrak{B}_k] \\ &= [\overline{\mathfrak{A}}_i, \mathfrak{B}_i] = [\overline{\mathfrak{A}}_i, \mathfrak{D}_i]\end{aligned}$$

kürzeste Darstellungen. Es kommt also:

$$\overline{\mathfrak{A}}_i \cdot \mathfrak{B}_i \equiv 0\,(\mathfrak{D}_i), \quad \overline{\mathfrak{A}}_i \not\equiv 0\,(\mathfrak{D}_i); \qquad \overline{\mathfrak{A}}_i \cdot \mathfrak{D}_i \equiv 0\,(\mathfrak{B}_i), \quad \overline{\mathfrak{A}}_i \not\equiv 0\,(\mathfrak{B}_i).$$

Da nun nach Satz VI die irreduziblen Ideale $\mathfrak{B}_i$ und $\mathfrak{D}_i$ primär sind, folgt daraus die Existenz zweier Zahlen λ_i und μ_i, derart, daß

$$\mathfrak{B}_i^{\lambda_i} \equiv 0\,(\mathfrak{D}_i); \qquad \mathfrak{D}_i^{\mu_i} \equiv 0\,(\mathfrak{B}_i). \tag{5}$$

Bezeichnen nun $\mathfrak{P}_i$ bzw. $\overline{\mathfrak{P}}_i$ die zugehörigen Primideale von $\mathfrak{B}_i$ bzw. $\mathfrak{D}_i$; also $\mathfrak{P}_i^{\varrho_i} \equiv 0\,(\mathfrak{B}_i)$; $\overline{\mathfrak{P}}_i^{\sigma_i} \equiv 0\,(\mathfrak{D}_i)$, so kommt nach (5):

$$\mathfrak{P}_i^{\lambda_i \varrho_i} \equiv 0\,(\overline{\mathfrak{P}}_i); \qquad \overline{\mathfrak{P}}_i^{\mu_i \sigma_i} \equiv 0\,(\mathfrak{P}_i),$$

und daraus nach der Eigenschaft der Primideale:

$$\mathfrak{P}_i \equiv 0\,(\overline{\mathfrak{P}}_i); \qquad \overline{\mathfrak{P}}_i \equiv 0\,(\mathfrak{P}_i); \qquad \mathfrak{P}_i = \overline{\mathfrak{P}}_i.$$

Damit ist bewiesen:

Satz VII. *Bei zwei verschiedenen kürzesten Darstellungen eines Ideals als kleinstes gemeinsames Vielfaches von irreduziblen Idealen stimmen die zugehörigen Primideale, unter denen auch gleiche*[20]) *und zwar bei jeder Zerlegung gleich oft auftreten können, überein. Die Ideale selbst lassen sich folglich auf mindestens eine Art derart paarweise zuordnen, daß jeweils eine Potenz des einen Ideals* $\mathfrak{B}_i$ *durch das zugeord-*

---

[20]) Das zeigt etwa das Beispiel von [19]):

$$(x^2, xy, y^\lambda) = [(x^2, y), (x, y^\lambda)],$$

wo $\lambda \geqq 2$. Die beiden zugehörigen Primideale sind hier: (x, y).

nete $\mathfrak{D}_i$ teilbar ist und umgekehrt. Ihre Anzahl stimmt nach Satz IV *überein*[21]).

§ 5.

Darstellung eines Ideals als kleinstes gemeinsames Vielfaches von größten primären Idealen. Eindeutigkeit der zugehörigen Primideale.

Definition IV. *Eine kürzeste Darstellung $\mathfrak{M} = [\mathfrak{Q}_1 \ldots \mathfrak{Q}_a]$ soll als kleinstes gemeinsames Vielfaches von größten primären Idealen bezeichnet werden, wenn alle $\mathfrak{Q}$ primär sind, aber das kleinste gemeinsame Vielfache zweier $\mathfrak{Q}$ nicht mehr primär ist.*

Daß mindestens eine solche Darstellung stets existiert, folgt aus der Darstellung von $\mathfrak{M}$ als kleinstes gemeinsames Vielfaches von irreduziblen Idealen. Denn diese Ideale sind primär; entweder liegt nun schon eine Darstellung durch größte primäre vor, oder aber das kleinste gemeinsame Vielfache irgend zweier Ideale wird wieder primär. Da hier die Anzahl der Ideale um eins abgenommen hat, führt die Wiederholung des Verfahrens nach endlich vielen Schritten zu der gewünschten Darstellung.

Diese Darstellung ist nach Hilfssatz IV reduziert. Umgekehrt entsteht jede reduzierte Darstellung durch größte primäre Ideale auf diese Art, wie die Auflösung der $\mathfrak{Q}$ in irreduzible Ideale zeigt.

Um hier aus Satz VII einen entsprechenden Eindeutigkeitssatz zu folgern, ist der Zusammenhang mit den zugehörigen Primidealen zu untersuchen nach

Satz VIII. *Besitzen die primären Ideale $\mathfrak{N}_1, \mathfrak{N}_2, \ldots, \mathfrak{N}_\lambda$ alle dasselbe zugehörige Primideal $\mathfrak{P}$, so ist auch ihr kleinstes gemeinsames Vielfaches $\mathfrak{Q} = [\mathfrak{N}_1, \mathfrak{N}_2, \ldots, \mathfrak{N}_\lambda]$ primär und hat $\mathfrak{P}$ zum zugehörigen Primideal. Ist umgekehrt $\mathfrak{Q} = [\mathfrak{N}_1 \ldots \mathfrak{N}_\lambda]$ eine reduzierte Darstellung für das primäre Ideal $\mathfrak{Q}$, so sind alle $\mathfrak{N}_i$ primär und besitzen als zugehöriges Primideal das zugehörige Primideal $\mathfrak{P}$ von $\mathfrak{Q}$.*

Zum Nachweis des ersten Teiles der Behauptung sei zunächst bemerkt, daß aus $\mathfrak{P}^{\varrho_i} \equiv 0\,(\mathfrak{N}_i)$ für jedes i auch folgt: $\mathfrak{P}^{\tau} \equiv 0\,(\mathfrak{Q})$, wo τ den größten der Indizes ϱ_i bedeutet. Da $\mathfrak{P}$ ferner auch Teiler von $\mathfrak{Q}$ ist, ist $\mathfrak{P}$ notwendig das zugehörige Primideal, wenn $\mathfrak{Q}$ primär ist. Aus

$$\mathfrak{A} \cdot \mathfrak{B} \equiv 0\,(\mathfrak{Q}); \qquad \mathfrak{B}^k \not\equiv 0\,(\mathfrak{Q}) \text{ (für jedes } k)$$

folgt somit $\mathfrak{B} \not\equiv 0\,(\mathfrak{P})$; also $\mathfrak{B}^k \not\equiv (\mathfrak{N}_i)$ (für jedes k);

und somit $\mathfrak{A} \equiv 0\,(\mathfrak{N}_i)$; also $\mathfrak{A} \equiv 0\,(\mathfrak{Q})$,

womit $\mathfrak{Q}$ als primär, $\mathfrak{P}$ als zugehöriges Primideal erwiesen ist.

---

[21]) Für die Eindeutigkeit der unter den irreduziblen Idealen enthaltenen „isolierten“ Ideale vgl. § 7.

Sei umgekehrt vorerst

$$\mathfrak{Q} = [\mathfrak{N}_1 \ldots \mathfrak{N}_\lambda] = [\mathfrak{N}_i, \mathfrak{L}_i]$$

eine kürzeste Darstellung von $\mathfrak{Q}$ durch *primäre* Ideale $\mathfrak{N}_i$ und seien jeweils $\mathfrak{P}_i$ die zugehörigen Primideale. Aus

$$\mathfrak{L}_i \cdot \mathfrak{N}_i \equiv 0 \,(\mathfrak{Q}); \qquad \mathfrak{L}_i \not\equiv 0 \,(\mathfrak{Q})$$

(wegen der kürzesten Darstellung) kommt dann:

$$\mathfrak{N}_i^{\sigma_i} \equiv 0 \,(\mathfrak{Q}); \text{ oder } \mathfrak{P}_i^{\varrho_i \sigma_i} \equiv 0 \,(\mathfrak{Q}).$$

Da $\mathfrak{P}_i$ zugleich Teiler von $\mathfrak{Q}$ ist, stimmt also $\mathfrak{P}_i$ für jedes i mit dem zugehörigen Primideal $\mathfrak{P}$ von $\mathfrak{Q}$ überein.

Es ist noch zu zeigen, daß bei *jeder reduzierten* Darstellung $\mathfrak{Q} = [\mathfrak{N}_1 \ldots \mathfrak{N}_\lambda]$ die $\mathfrak{N}_i$ primär sind[22]). Dazu löse man die $\mathfrak{N}_i$ in ihre irreduziblen Ideale $\mathfrak{B}$ auf; in der so entstehenden *kürzesten* Darstellung $\mathfrak{Q} = [\mathfrak{B}_1 \ldots \mathfrak{B}_\mu]$ ist dann jedes Ideal primär und besitzt nach dem eben Bewiesenen $\mathfrak{P}$ als zugehöriges Primideal. Dann gilt aber nach dem oben bewiesenen ersten Teil des Satzes das gleiche für jedes $\mathfrak{N}_i$, womit *Satz* VIII *vollständig bewiesen ist.*

Zusatz. Hieraus folgt noch, daß ein *Primideal notwendig irreduzibel* ist. Denn aus der reduzierten Darstellung $\mathfrak{P} = [\mathfrak{N}, \mathfrak{L}]$ kommt nach Satz VIII: $\mathfrak{N} \equiv 0 \,(\mathfrak{P})$; also wegen $\mathfrak{P} \equiv 0 \,(\mathfrak{N})$ auch $\mathfrak{P} = \mathfrak{N}$ und ebenso $\mathfrak{P} = \mathfrak{L}$. Die Irreduzibilität von $\mathfrak{P}$ ergibt sich auch direkt: denn aus $\mathfrak{P} = [\mathfrak{N}, \mathfrak{L}]$ folgt: $\mathfrak{N} \cdot \mathfrak{L} \equiv 0 \,(\mathfrak{P})$; $\mathfrak{N} \not\equiv (\mathfrak{P})$; $\mathfrak{L} \not\equiv 0 \,(\mathfrak{P})$ im Widerspruch zu der Definitionseigenschaft des Primideals.

Seien jetzt

$$\mathfrak{M} = [\mathfrak{Q}_1 \ldots \mathfrak{Q}_\alpha] = [\bar{\mathfrak{Q}}_1 \ldots \bar{\mathfrak{Q}}_\beta]$$

zwei reduzierte Darstellungen von $\mathfrak{M}$ als kleinstes gemeinsames Vielfaches von größten primären Idealen. Indem man die $\mathfrak{Q}$ in ihre irreduziblen Ideale $\mathfrak{B}$, die $\bar{\mathfrak{Q}}$ entsprechend in die irreduziblen Ideale $\mathfrak{D}$ auflöst, kommen zwei reduzierte Darstellungen für $\mathfrak{M}$ als kleinstes gemeinsames Vielfaches von irreduziblen Idealen, bei denen nach Satz VII sowohl die Anzahl der Komponenten wie die zugehörigen Primideale übereinstimmen. Nach Satz VIII besitzen dabei alle bei einem festem $\mathfrak{Q}_i$ auftretenden irreduziblen Ideale $\mathfrak{B}$ *dasselbe zugehörige Primideal* $\mathfrak{P}_i$; während das zu $\mathfrak{Q}_k$ gehörige $\mathfrak{P}_k$ notwendig davon verschieden ist, da sonst nach Satz VIII keine Darstellung

---

[22]) Daß hier die reduzierte Darstellung wesentlich ist, zeigt das Beispiel der nicht-reduzierten Darstellung: $\mathfrak{Q} = [x^2, xy, y^\lambda] = [(x^2, xy, y^2, yz), (x, y^\lambda)]$, wo $\lambda \geqq 2$. Hier ist $(x^2, xy, y^2, yz) = [(x^2, y), (x, y^2, z)]$ nach dem oben Bewiesenen nicht primär; denn letztere Darstellung ist eine kürzeste durch primäre Ideale, aber die zugehörigen Primideale (x, y) und (x, y, z) sind verschieden. ($\mathfrak{Q}$ ist nach [19]) primär.)

durch größte primäre Ideale vorläge. Die Anzahl α der $\mathfrak{Q}$ ist also gleich der Anzahl der verschiedenen zugehörigen Primideale $\mathfrak{P}$ der $\mathfrak{B}$; diese verschiedenen $\mathfrak{P}$ bilden die zugehörigen Primideale der $\mathfrak{Q}$. Das gleiche gilt von den $\bar{\mathfrak{Q}}$ in bezug auf ihre Auflösung in die $\mathfrak{D}$. Aus Satz VII folgt also die *Anzahlgleichheit der $\mathfrak{Q}$ und $\bar{\mathfrak{Q}}$*, und das *Übereinstimmen ihrer zugehörigen Primideale.* Zugleich zeigt sich, daß die am Anfang des Paragraphen angegebene Zusammenfassung der irreduziblen Ideale zu größten primären darin besteht, alle mit demselben zugehörigen Primideal, und nur diese, zusammenzufassen. Satz VIII zeigt weiter die Irreduzibilitätseigenschaft der größten primären Ideale: Sie lassen keine reduzierte Darstellung als kleinstes gemeinsames Vielfaches von größten primären zu.

Zusamenfassend ist bewiesen:

Satz IX. *Bei zwei reduzierten Darstellungen eines Ideals als kleinstes gemeinsames Vielfaches von größten primären Idealen stimmen die Anzahl der Komponenten und die zugehörigen Primideale, die alle voneinander verschieden sind, überein.* M. a. W.: *Jedem $\mathfrak{Q}$ läßt sich eindeutig ein $\bar{\mathfrak{Q}}$ zuordnen, derart, daß eine Potenz von $\mathfrak{Q}$ durch $\bar{\mathfrak{Q}}$ teilbar ist, und umgekehrt*[23]. — *Die $\mathfrak{Q}$ und $\bar{\mathfrak{Q}}$ haben Irreduzibilitätseigenschaft in bezug auf die Zerlegung in größte primäre Ideale.*

Zusatz. Es sei bemerkt, daß Satz IX im wesentlichen erhalten bleibt, wenn man anstatt reduzierter nur *kürzeste* Darstellung voraussetzt. Ist dann etwa $\mathfrak{M} = [\mathfrak{Q}_1 \ldots \mathfrak{Q}_i^* \ldots \mathfrak{Q}_\alpha]$ reduziert in bezug auf $\mathfrak{Q}_i^*$, und $\mathfrak{Q}_i^*$ ein echter Teiler von $\mathfrak{Q}_i$, $\mathfrak{L}_i$ das Komplement von $\mathfrak{Q}_i$, so kommt nach Hilfssatz IV: $\mathfrak{Q}_i = [\mathfrak{Q}_i^*, (\mathfrak{L}_i, \mathfrak{Q}_i)]$; und diese Darstellung ist reduziert in bezug auf $\mathfrak{Q}_i^*$. Nach Satz VIII, bei dessen Anwendung nötigenfalls $(\mathfrak{L}_i, \mathfrak{Q}_i)$ durch einen echten Teiler zu ersetzen ist, ist also $\mathfrak{Q}_i^*$ primär und hat dasselbe zugehörige Primideal $\mathfrak{P}_i$ wie $\mathfrak{Q}_i$. Die Fortsetzung des Verfahrens zeigt, daß jeder solchen Darstellung eine reduzierte durch größte primäre Ideale zugeordnet werden kann, derart, daß die Anzahl der Komponenten und die zugehörigen Primideale übereinstimmen. *Es gilt also auch bei kürzester Darstellung, daß bei zwei verschiedenen Darstellungen die Anzahl der Komponenten und die zugehörigen Primideale übereinstimmen.*

Die derart *eindeutig* definierten zugehörigen, voneinander verschiedenen Primideale sollen kurz als „*die zugehörigen Primideale von $\mathfrak{M}$*“ bezeichnet werden.

---

[23]) Ein Beispiel verschiedener Darstellungen ist das in [12]) zu Satz II gegebene: $(x^2, xy) = [(x), (x^2, \mu x + y)]$ für beliebiges μ. Da die zugehörigen Primideale $\mathfrak{P}_1 = (x)$; $\mathfrak{P}_2 = (x, y)$ voneinander verschieden sind, handelt es sich um größte primäre Ideale. — Für die Eindeutigkeit der „isolierten“ größten primären Ideale vgl. § 7.

§ 6.

Eindeutige Darstellung eines Ideals als kleinstes gemeinsames Vielfaches von relativprim-irreduziblen Idealen.

Definition V. *Ein Ideal* $\mathfrak{R}$ *heißt relativprim zu* $\mathfrak{S}$, *wenn aus* $\mathfrak{T}\cdot\mathfrak{R}\equiv 0\,(\mathfrak{S})$ *notwendig folgt:* $\mathfrak{T}\equiv 0\,(\mathfrak{S})$. *Ist sowohl* $\mathfrak{R}$ *zu* $\mathfrak{S}$, *wie* $\mathfrak{S}$ *zu* $\mathfrak{R}$ *relativprim, so heißen* $\mathfrak{R}$ *und* $\mathfrak{S}$ *gegenseitig relativprim*[24]). *Ein Ideal heißt relativprim-irreduzibel, wenn es sich nicht als kleinstes gemeinsames Vielfaches von gegenseitig relativprimen echten Teilern darstellen läßt.*

Nimmt man insbesondere anstatt $\mathfrak{T}$ den größten gemeinsamen Teiler $\mathfrak{T}_0$ aller $\mathfrak{T}$, für die $\mathfrak{T}\cdot\mathfrak{R}\equiv 0\,(\mathfrak{S})$, so wird auch $\mathfrak{T}_0\cdot\mathfrak{R}\equiv 0\,(\mathfrak{S})$ und $\mathfrak{S}\equiv 0\,(\mathfrak{T}_0)$. Es wird also $\mathfrak{T}_0=\mathfrak{S}$, wenn $\mathfrak{R}$ relativprim zu $\mathfrak{S}$; $\mathfrak{T}_0$ ein echter Teiler von $\mathfrak{S}$, wenn $\mathfrak{R}$ nicht relativprim zu $\mathfrak{S}$[25]).

Dem Eindeutigkeitsbeweis liegt zugrunde

Satz X. 1. *Ist* $\mathfrak{R}$ *relativprim zu den Idealen* $\mathfrak{S}_1\ldots\mathfrak{S}_\lambda$, *so ist* $\mathfrak{R}$ *auch relativprim zu ihrem kleinsten gemeinsamen Vielfachen* $\mathfrak{S}$.

2. *Sind die Ideale* $\mathfrak{S}_1\ldots\mathfrak{S}_\lambda$ *relativprim zu* $\mathfrak{R}$, *so ist auch ihr kleinstes gemeinsames Vielfaches* $\mathfrak{S}$ *relativprim zu* $\mathfrak{R}$.

3. *Ist* $\mathfrak{R}$ *relativprim zu* $\mathfrak{S}$ *und ist* $\mathfrak{S}=[\mathfrak{S}_1\ldots\mathfrak{S}_i]$ *eine reduzierte Darstellung für* $\mathfrak{S}$, *so ist* $\mathfrak{R}$ *auch relativprim zu jedem* $\mathfrak{S}_i$.

4. *Ist* $\mathfrak{S}$ *relativprim zu* $\mathfrak{R}$, *so ist auch jeder Teiler* $\mathfrak{S}_i$ *von* $\mathfrak{S}$ *relativprim zu* $\mathfrak{R}$.

1. Da aus $\mathfrak{T}\cdot\mathfrak{R}\equiv 0\,(\mathfrak{S})$ notwendig folgt: $\mathfrak{T}\cdot\mathfrak{R}\equiv 0\,(\mathfrak{S}_i)$, so wird nach Voraussetzung: $\mathfrak{T}\equiv 0\,(\mathfrak{S}_i)$ und damit $\mathfrak{T}\equiv 0\,(\mathfrak{S})$.

2. Es sei $\mathfrak{C}_1=[\mathfrak{S}_2\ldots\mathfrak{S}_\lambda]$; $\mathfrak{C}_{12}=[\mathfrak{S}_3\ldots\mathfrak{S}_\lambda]$; $\ldots$; $\mathfrak{C}_{12\ldots\lambda-1}=\mathfrak{S}_\lambda$ gesetzt. Aus $\mathfrak{T}\cdot\mathfrak{S}\equiv 0\,(\mathfrak{R})$ folgt dann $\mathfrak{T}\cdot\mathfrak{C}_1\cdot\mathfrak{S}_1\equiv 0\,(\mathfrak{R})$; also nach Voraussetzung: $\mathfrak{T}\cdot\mathfrak{C}_1\equiv 0\,(\mathfrak{R})$. Daraus folgt wieder: $\mathfrak{T}\cdot\mathfrak{C}_{12}\cdot\mathfrak{S}_2\equiv 0\,(\mathfrak{R})$; also nach Voraussetzung $\mathfrak{T}\cdot\mathfrak{C}_{12}\equiv 0\,(\mathfrak{R})$, und schließlich: $\mathfrak{T}\cdot\mathfrak{C}_{12\ldots\lambda-1}=\mathfrak{T}\cdot\mathfrak{S}_\lambda\equiv 0\,(\mathfrak{R})$; also $\mathfrak{T}\equiv 0\,(\mathfrak{R})$.

3. Es bedeute $\mathfrak{C}_i$ das Komplement von $\mathfrak{S}_i$; aus $\mathfrak{T}_0\cdot\mathfrak{R}\equiv 0\,(\mathfrak{S}_i)$ folgt dann wegen $\mathfrak{C}_i\cdot\mathfrak{R}\equiv 0\,(\mathfrak{C}_i)$ auch $[\mathfrak{T}_0,\mathfrak{C}_i]\cdot\mathfrak{R}\equiv 0\,(\mathfrak{S})$.

Wäre nun $\mathfrak{T}_0$ ein echter Teiler von $\mathfrak{S}_i$, so wäre wegen der reduzierten Darstellung $\mathfrak{S}=[\mathfrak{S}_i,\mathfrak{C}_i]$ auch $[\mathfrak{T}_0,\mathfrak{C}_i]$ ein echter Teiler von $\mathfrak{S}$ gegen die Voraussetzung.

---

[24]) Die Bedingung des relativprim ist nicht symmetrisch. Z. B. ist $\mathfrak{R}=(x^2,y)$ relativprim zu $\mathfrak{S}=(x)$; aber $\mathfrak{S}$ ist nicht relativprim zu $\mathfrak{R}$, da $\mathfrak{S}^2\equiv 0\,(\mathfrak{R})$, aber $\mathfrak{T}=\mathfrak{S}\not\equiv 0\,(\mathfrak{R})$ wird.

[25]) Dieses so definierte $\mathfrak{T}_0$ stimmt überein mit dem „Residualmodul" von Lasker; und in seiner Ausdehnung auf Zahlenmoduln statt Ideale mit dem „Quotient" zweier Moduln bei Dedekind. Lasker, a. a. O. S. 49, Dedekind (Zahlentheorie), S. 504.

4. Aus $\mathfrak{T}_0 \cdot \mathfrak{S}_i \equiv 0\,(\mathfrak{R})$, wo $\mathfrak{T}_0$ ein echter Teiler von $\mathfrak{R}$, folgt auch $\mathfrak{T}_0 \cdot \mathfrak{S} \equiv 0\,(\mathfrak{R})$; also wäre $\mathfrak{T}_0$ echter Teiler von $\mathfrak{R}$ gegen die Voraussetzung.

Definition V zeigt insbesondere, daß jedes Ideal relativprim zu dem aus *allen* Elementen von Σ bestehenden *Einheitsideal* $\mathfrak{O}$ wird[26]); die folgenden Sätze gelten aber nur für von $\mathfrak{O}$ verschiedene Ideale.

Aus dem eben bewiesenen Satz X ergibt sich zunächst

Hilfssatz V. *Jede Darstellung eines Ideals als kleinstes gemeinsames Vielfaches von gegenseitig relativprimen, von $\mathfrak{O}$ verschiedenen Idealen ist reduziert.*

Sei $\mathfrak{M} = [\mathfrak{R}_1\, \mathfrak{R}_2 \ldots \mathfrak{R}_\sigma] = [\mathfrak{R}_i, \mathfrak{L}_i]$ eine solche Darstellung. Nach Satz X, 2 ist dann auch $\mathfrak{L}_i$ relativprim zu $\mathfrak{R}_i$; $\mathfrak{R}_i$ kann also nicht in $\mathfrak{L}_i$ aufgehen; die Darstellung wird eine kürzeste. Denn aus $\mathfrak{L}_i \equiv 0\,(\mathfrak{R}_i)$, wo $\mathfrak{L}_i$ relativprim zu $\mathfrak{R}_i$, würde wegen $\mathfrak{O} \cdot \mathfrak{L}_i \equiv 0\,(\mathfrak{R}_i)$ auch folgen: $\mathfrak{O} \equiv 0\,(\mathfrak{R}_i)$; also $\mathfrak{R}_i = \mathfrak{O}$, was nach Voraussetzung ausgeschlossen ist. Sei nun $\mathfrak{R}_i$ durch den echten Teiler $\mathfrak{R}_i^*$ ersetzbar, dann wird nach Hilfssatz II $\mathfrak{R}_i$ reduzibel und es kommt: $\mathfrak{R}_i = [\mathfrak{R}_i^*, (\mathfrak{R}_i, \mathfrak{L}_i)]$. Ersetzt man hier gegebenenfalls $(\mathfrak{R}_i, \mathfrak{L}_i)$ durch einen echten Teiler $(\mathfrak{R}_i, \mathfrak{L}_i)^*$, ebenso $\mathfrak{R}_i^*$ durch einen echten Teiler, so daß eine reduzierte Darstellung für $\mathfrak{R}_i$ entsteht, so zeigt Satz X, 3, daß $\mathfrak{L}_i$ auch relativprim zu $(\mathfrak{R}_i, \mathfrak{L}_i)^*$ wird, und dieses ist wegen der kürzesten Darstellung von $\mathfrak{O}$ verschieden. Da aber $(\mathfrak{R}_i, \mathfrak{L}_i)^*$ in $(\mathfrak{R}_i, \mathfrak{L}_i)$ und $(\mathfrak{R}_i, \mathfrak{L}_i)$ in $\mathfrak{L}_i$ aufgeht, ist damit ein Widerspruch nachgewiesen.

Aus Satz X ergibt sich ferner der den Zusammenhang mit den zugehörigen Primidealen vermittelnde

Satz XI. *Ist $\mathfrak{R}$ relativprim zu $\mathfrak{S}$ und $\mathfrak{S}$ von $\mathfrak{O}$ verschieden, so ist kein zugehöriges Primideal von $\mathfrak{R}$*[27]) *durch ein zugehöriges Primideal von $\mathfrak{S}$ teilbar. Findet umgekehrt keine solche Teilbarkeit statt, so ist $\mathfrak{R}$ relativprim zu $\mathfrak{S}$, und natürlich $\mathfrak{S}$ von $\mathfrak{O}$ verschieden.*

Seien

$$\mathfrak{R} = [\mathfrak{Q}_1 \ldots \mathfrak{Q}_\alpha], \qquad \mathfrak{S} = [\mathfrak{Q}_1^* \ldots \mathfrak{Q}_\beta^*]$$

reduzierte Darstellungen von $\mathfrak{R}$ und $\mathfrak{S}$ durch größte primäre Ideale; $\mathfrak{P}_1 \ldots \mathfrak{P}_\alpha$, $\mathfrak{P}_1^* \ldots \mathfrak{P}_\beta^*$ die zugehörigen Primideale. Wir zeigen die Behauptung in der Form: Ist ein $\mathfrak{P}$ durch ein $\mathfrak{P}^*$ teilbar, so kann $\mathfrak{R}$ nicht relativprim zu $\mathfrak{S}$ sein, und umgekehrt.

Sei also $\mathfrak{P}_\mu \equiv 0\,(\mathfrak{P}_\nu^*)$ und folglich auch: $\mathfrak{Q}_\mu \equiv 0\,(\mathfrak{P}_\nu^*)$, woraus nach Definition von $\mathfrak{P}_\nu^*$ folgt: $\mathfrak{Q}_\mu^{\sigma_\nu} \equiv 0\,(\mathfrak{Q}_\nu^*)$, also auch $\mathfrak{R}^{\sigma_\nu} \equiv 0\,(\mathfrak{Q}_\nu^*)$. Es sei

---

[26]) $\mathfrak{O}$ spielt nur in bezug auf Teilbarkeit und kleinstes gemeinsames Vielfaches, nicht in bezug auf Produktbildung die Rolle der Einheit. Es wird etwa $\mathfrak{O} = (x)$ für den Bereich aller ganzzahligen Polynome von x ohne konstantes Glied; $\mathfrak{O} = (2)$ für den Bereich aller geraden Zahlen.

[27]) Definition der zugehörigen Primideale von $\mathfrak{R}$ in § 5, Schluß.

nun $\mathfrak{R}^\tau$ die niedrigste Potenz von $\mathfrak{R}$, die durch $\mathfrak{Q}_\nu^*$ teilbar ist. Für $\tau = 1$ wird $\mathfrak{R}$ durch $\mathfrak{Q}_\nu^*$ teilbar; da aber nach Voraussetzung $\mathfrak{S}$ von $\mathfrak{O}$ verschieden, wird $\mathfrak{R}$ also nicht relativprim zu $\mathfrak{Q}_\nu^*$. Für $\tau \geqq 2$ wird $\mathfrak{R}^{\tau-1} \cdot \mathfrak{R} \equiv 0 (\mathfrak{Q}_\nu^*)$, $\mathfrak{R}^{\tau-1} \not\equiv 0 (\mathfrak{Q}_\nu^*)$, also $\mathfrak{R}$ *nicht relativprim zu* $\mathfrak{Q}_\nu^*$[28]); und *folglich* ist in beiden Fällen nach Satz X, 3 auch $\mathfrak{R}$ nicht relativprim zu $\mathfrak{S}$.

Ist umgekehrt $\mathfrak{R}$ nicht relativprim zu $\mathfrak{S}$, so ist nach Satz X, 1 auch $\mathfrak{R}$ nicht relativprim zu mindestens einem $\mathfrak{Q}_\nu^*$. Es gilt also: $\mathfrak{T}_0 \cdot \mathfrak{R} \equiv 0 (\mathfrak{Q}_\nu^*)$; $\mathfrak{T}_0 \not\equiv 0 (\mathfrak{Q}_\nu^*)$, und daraus, da $\mathfrak{Q}_\nu^*$ primär ist: $\mathfrak{R}^\tau \equiv 0 (\mathfrak{Q}_\nu^*)$, also auch $\mathfrak{Q}_1^\tau \ldots \mathfrak{Q}_\alpha^\tau \equiv 0 (\mathfrak{Q}_\nu^*)$. Daraus folgt aber für die zugehörigen Primideale: $\mathfrak{P}_1^{\tau\varrho_1} \ldots \mathfrak{P}_\alpha^{\tau\varrho_\alpha} \equiv 0 (\mathfrak{P}_\nu^*)$; und nach der Eigenschaft der Primideale geht folglich $\mathfrak{P}_\nu^*$ in mindestens einem $\mathfrak{P}$ auf, womit *Satz* XI *bewiesen* ist.

Aus Satz X und XI ergibt sich nun die *Existenz*[29]) *und Eindeutigkeit der Zerlegung in relativprim-irreduzible Ideale* wie folgt:

Sei $\mathfrak{M} = [\mathfrak{Q}_1 \ldots \mathfrak{Q}_\alpha]$ eine reduzierte (oder wenigstens kürzeste) Darstellung von $\mathfrak{M}$ durch größte primäre Ideale; $\mathfrak{P}_1 \ldots \mathfrak{P}_\alpha$ die zugehörigen Primideale. Wir fassen die $\mathfrak{P}$ derart in Gruppen zusammen, daß *kein Ideal einer Gruppe teilbar wird durch ein Ideal einer davon verschiedenen Gruppe, während die einzelne Gruppe sich nicht in zwei Teilgruppen spalten läßt, denen beiden diese Eigenschaft zukommt.* Um eine solche Gruppeneinteilung zu konstruieren, ist zu bemerken, daß nach Definition die einzelne Gruppe G neben jedem Ideal $\mathfrak{P}$ auch alle seine in $\mathfrak{P}_1 \ldots \mathfrak{P}_\alpha$ vorkommenden Teiler und Vielfachen (d. h. durch $\mathfrak{P}$ teilbaren) enthalten muß. Seien etwa $\mathfrak{P}^{(i_1)}$ alle Vielfachen von $\mathfrak{P}$, $\mathfrak{P}_{j_1}^{(i_1)}$ alle Teiler von $\mathfrak{P}^{(i_1)}$, $\mathfrak{P}_{j_1}^{(i_1 i_2)}$ alle Vielfachen von $\mathfrak{P}_{j_1}^{(i_1)}$ usf.; allgemein $\mathfrak{P}_{j_1 \ldots j_{\lambda-1}}^{(i_1 \ldots i_\lambda)}$ alle Vielfachen von $\mathfrak{P}_{j_1 \ldots j_{\lambda-1}}^{(i_1 \ldots i_{\lambda-1})}$, $\mathfrak{P}_{j_1 \ldots j_\lambda}^{(i_1 \ldots i_\lambda)}$ alle Teiler von $\mathfrak{P}_{j_1 \ldots j_{\lambda-1}}^{(i_1 \ldots i_\lambda)}$. Da es sich im ganzen nur um endlich viele Ideale $\mathfrak{P}$ handelt, muß das Verfahren nach endlich vielen Schritten abbrechen; d. h. kein von allen vorangehenden verschiedenes Ideal liefern. Der so gewonnene Inbegriff von Idealen $\mathfrak{P}$ bildet nun tatsächlich eine Gruppe G von den gewünschten Eigenschaften.

Denn nach Definition enthält G neben jedem $\mathfrak{P}_{j_1 \ldots j_{\lambda-1}}^{(i_1 \ldots i_{\lambda-1})}$ auch alle Vielfachen $\mathfrak{P}_{j_1 \ldots j_{\lambda-1}}^{(i_1 \ldots i_\lambda)}$, neben jedem $\mathfrak{P}_{j_1 \ldots j_{\lambda-1}}^{(i_1 \ldots i_\lambda)}$ auch alle Teiler $\mathfrak{P}_{j_1 \ldots j_\lambda}^{(i_1 \ldots i_\lambda)}$. Darunter sind aber auch alle Teiler der $\mathfrak{P}_{j_1 \ldots j_{\lambda-1}}^{(i_1 \ldots i_{\lambda-1})}$ enthalten, während

---

[28]) $\mathfrak{R}^0$ ist nicht definiert, da Σ die Einheit nicht zu enthalten braucht; daher mußte der Fall $\tau = 1$ vorweggenommen werden. $\tau = 0$ ist auch in dem Fall, wo Σ eine Einheit enthält, durch die Voraussetzung über $\mathfrak{S}$ ausgeschlossen.

[29]) Die Existenz der Zerlegung läßt sich auch direkt beweisen, in genauer Analogie mit der in § 2 nachgewiesenen Existenz der Zerlegung in endlich viele irreduzible Ideale.

die Vielfachen der $\mathfrak{P}_{j_1 \ldots j_{\lambda-1}}^{(i_1 \ldots i_\lambda)}$ selbst wieder $\mathfrak{P}_{j_1 \ldots j_{\lambda-1}}^{(i_1 \ldots i_\lambda)}$ sind. Die nicht in G enthaltenen Ideale können also weder Teiler noch Vielfache der in G enthaltenen sein. G erfüllt aber auch die Irreduzibilitätsbedingung. Denn liegt eine Einteilung in zwei Teilgruppen $G^{(1)}$ und $G^{(2)}$ vor, und enthält $G^{(1)}$ etwa $\mathfrak{P}_{j_1 \ldots j_\lambda}^{(i_1 \ldots i_\lambda)}$ $\left(\text{bzw. } \mathfrak{P}_{j_1 \ldots j_{\lambda-1}}^{(i_1 \ldots i_\lambda)}\right)$, so enthält es auch alle vorangehenden, da diese abwechselnd Vielfache und Teiler (bzw. Teiler und Vielfache) sind, also auch $\mathfrak{P}$ und damit die ganze Gruppe G. Verfährt man mit den nicht in G enthaltenen Idealen entsprechend, so kommt damit eine Gruppeneinteilung $G_1 \ldots G_\sigma$ aller $\mathfrak{P}$, der die gewünschten Eigenschaften zukommen. Eine solche *Gruppeneinteilung ist eindeutig;* denn sei $G_1' \ldots G_\tau'$ eine zweite Einteilung und $\mathfrak{P}_{j_1 \ldots j_\lambda}^{(i_1 \ldots i_\lambda)}$ $\left(\text{bzw. } \mathfrak{P}_{j_1 \ldots j_{\lambda-1}}^{(i_1 \ldots i_\lambda)}\right)$ ein Element von G_i', so enthält nach dem obigen G_i' die ganze Gruppe G und ist also wegen der Irreduzibilitätseigenschaft mit G identisch.

Bedeuten nun $\mathfrak{P}_{i\mu}$ (wo μ von 1 bis λ_i läuft), die in einer Gruppe G_i zusammengefaßten Ideale $\mathfrak{P}$, so sind, da die $\mathfrak{P}$ alle voneinander verschieden sind, die einer kürzesten Darstellung entsprechenden primären Ideale $\mathfrak{Q}_{i\mu}$ eindeutig bestimmt. Setzen wir

$$\mathfrak{R}_i = [\mathfrak{Q}_{i1} \ldots \mathfrak{Q}_{i\lambda_i}], \text{ so kommt } \mathfrak{M} = [\mathfrak{R}_1 \ldots \mathfrak{R}_\sigma];$$

wir zeigen, daß dadurch eine *Zerlegung von $\mathfrak{M}$ in relativprim-irreduzible Ideale* erreicht ist. Zunächst ist zu bemerken, daß Satz XI anwendbar bleibt, auch wenn $\mathfrak{R}_i = [\mathfrak{Q}_{i_1} \ldots \mathfrak{Q}_{i\lambda_i}]$ nur eine kürzeste Darstellung ist, da nach dem Zusatz zu Satz IX die zugehörigen Primideale dadurch schon eindeutig definiert sind. Da nun kein zugehöriges Primideal $\mathfrak{P}_{i\mu}$ von $\mathfrak{R}_i$ durch ein zugehöriges Primideal $\mathfrak{P}_{j\nu}$ von $\mathfrak{R}_j$ teilbar ist, und umgekehrt, sind nach Satz XI $\mathfrak{R}_i$ und $\mathfrak{R}_j$ gegenseitig relativprim; und jedes einzelne $\mathfrak{R}_i$ ist nach Satz XI wegen der Irreduzibilitätseigenschaft der Gruppe G_i relativprim-irreduzibel, da bei Reduzibilität stets von $\mathfrak{D}$ verschiedene Ideale in Betracht kommen. Nach Hilfssatz V handelt es sich ferner um eine reduzierte Darstellung, auch wenn man ursprünglich nur von einer kürzesten Darstellung durch die $\mathfrak{Q}$ ausgegangen war. Umgekehrt führt nach Satz XI jede Zerlegung in relativprim-irreduzible Ideale auf die angegebene Gruppeneinteilung der $\mathfrak{P}_{i\mu}$.

Sei nun $\mathfrak{M} = [\overline{\mathfrak{R}}_1 \ldots \overline{\mathfrak{R}}_\tau]$ eine *zweite Darstellung von $\mathfrak{M}$ durch relativprim-irreduzible Ideale,* die nach Hilfssatz V reduziert ist. Da dann, wie die Auflösung der $\overline{\mathfrak{R}}$ in größte primäre Ideale zeigt, die zugehörigen Primideale übereinstimmen, stimmen also auch die Gruppeneinteilungen dieser Primideale, deren Eindeutigkeit oben bewiesen, überein. Es wird somit $\tau = \sigma$; und die Bezeichnung läßt sich so wählen, daß

$\mathfrak{R}_i$, $\overline{\mathfrak{R}_i}$ zu derselben Gruppe gehören. Sei dann

$$\mathfrak{M} = [\mathfrak{R}_i, \mathfrak{L}_i] = [\overline{\mathfrak{R}_i}, \overline{\mathfrak{L}_i}]$$

die Darstellung durch Ideal und Komplement. Dann wird, da $\overline{\mathfrak{R}_i}$ derselben Gruppe zugeordnet ist wie $\mathfrak{R}_i$, nach Satz XI auch $\mathfrak{L}_i$ *relativprim zu* $\overline{\mathfrak{R}_i}$, und $\overline{\mathfrak{L}_i}$ *relativprim zu* $\mathfrak{R}_i$. Wegen

$$\mathfrak{R}_i \cdot \mathfrak{L}_i \equiv 0\,(\overline{\mathfrak{R}_i}), \qquad \overline{\mathfrak{R}_i} \cdot \overline{\mathfrak{L}_i} \equiv 0\,(\mathfrak{R}_i)$$

kommt somit

$$\mathfrak{R}_i \equiv 0\,(\overline{\mathfrak{R}_i}); \qquad \overline{\mathfrak{R}_i} \equiv 0\,(\mathfrak{R}_i); \qquad \mathfrak{R}_i = \overline{\mathfrak{R}_i}.$$

Damit ist bewiesen:

Satz XII. *Jedes Ideal läßt sich eindeutig darstellen als kleinstes gemeinsames Vielfaches von endlich vielen gegenseitig relativprimen und relativprim-irreduziblen Idealen.*

§ 7.

Eindeutigkeit der isolierten Ideale.

Definition VI. *Ist die kürzeste Darstellung* $\mathfrak{M} = [\mathfrak{R}, \mathfrak{L}]$ *reduziert in bezug auf* $\mathfrak{L}$, *so heißt* $\mathfrak{R}$ *isoliertes Ideal, wenn kein zugehöriges Primideal von* $\mathfrak{R}$ *in einem zugehörigen Primideal von* $\mathfrak{L}$ *aufgeht,* m. a. W., *wenn* $\mathfrak{L}$ *relativ prim zu* $\mathfrak{R}$ *ist.*

Danach erfüllt die Darstellung $\mathfrak{M} = [\mathfrak{R}, \mathfrak{L}]$ die Bedingungen der Darstellung $\mathfrak{M} = [\mathfrak{R}_i, \mathfrak{L}_i]$ in Hilfssatz V, und mit Hilfssatz V ist bewiesen:

Hilfssatz VI. *Ist* $\mathfrak{R}$ *isoliertes Ideal der in bezug auf* $\mathfrak{L}$ *reduzierten, kürzesten Darstellung* $\mathfrak{M} = [\mathfrak{R}, \mathfrak{L}]$, *so ist die Darstellung auch reduziert in bezug auf* $\mathfrak{R}$.

Da es sich also bei isolierten Idealen um reduzierte Darstellung handelt, ergänzen sich die bei der Zerlegung von $\mathfrak{R}$ und $\mathfrak{L}$ in *irreduzible* Ideale auftretenden zugehörigen Primideale zu den eindeutig bestimmten, bei der entsprechenden Zerlegung von $\mathfrak{M}$ auftretenden zugehörigen Primidealen.

Es geht somit kein zu der Zerlegung in irreduzible Ideale gehöriges Primideal von $\mathfrak{R}$ in den übrigen, zu der entsprechenden Zerlegung von $\mathfrak{M}$ gehörigen Primidealen auf. Ist umgekehrt diese Bedingung erfüllt, und tritt $\mathfrak{R}$ in mindestens einer in bezug auf $\mathfrak{R}$ reduzierten Darstellung $\mathfrak{M} = [\mathfrak{R}, \mathfrak{L}]$, also auch in einer reduzierten Darstellung $\mathfrak{M} = [\mathfrak{R}, \mathfrak{L}^*]$ auf, so ist $\mathfrak{R}$ nach Definition VI isoliert. Daraus ergibt sich die von dem speziellen Komplement $\mathfrak{L}$ unabhängige

Definition VIa. $\mathfrak{R}$ *heißt isoliertes Ideal, wenn die zu der Zerlegung in irreduzible Ideale gehörigen Primideale von* $\mathfrak{R}$ *nicht in den*

übrigen, zu der entsprechenden Zerlegung von $\mathfrak{M}$ *gehörigen Primidealen aufgehen, und wenn* $\mathfrak{R}$ *in mindestens einer in bezug auf* $\mathfrak{R}$ *reduzierten Darstellung* $\mathfrak{M} = [\mathfrak{R}, \mathfrak{Q}]$ *auftritt*[30]).

Seien nun

$$\mathfrak{M} = [\mathfrak{R}, \mathfrak{Q}] = [\overline{\mathfrak{R}}, \overline{\mathfrak{Q}}]$$

zwei Darstellungen von $\mathfrak{M}$ durch isolierte Ideale $\mathfrak{R}$ und $\overline{\mathfrak{R}}$ und Komplemente $\mathfrak{Q}$ und $\overline{\mathfrak{Q}}$; derart, daß die zugehörigen Primideale von $\mathfrak{R}$ und $\overline{\mathfrak{R}}$ übereinstimmen. Ersetzt man $\mathfrak{Q}$ und $\overline{\mathfrak{Q}}$ durch solche Teiler $\mathfrak{Q}^*$ und $\overline{\mathfrak{Q}}^*$, daß die Darstellungen reduziert werden, so stimmen also auch die zugehörigen Primideale von $\mathfrak{Q}^*$ und $\overline{\mathfrak{Q}}^*$ überein; nach Satz XI wird also $\mathfrak{Q}^*$ relativprim zu $\overline{\mathfrak{R}}$, $\overline{\mathfrak{Q}}^*$ relativprim zu $\mathfrak{R}$. Wegen

$$\mathfrak{R} \cdot \mathfrak{Q}^* \equiv 0\,(\overline{\mathfrak{R}}); \qquad \overline{\mathfrak{R}}\,\overline{\mathfrak{Q}}^* \equiv 0\,(\mathfrak{R})$$

kommt somit

$$\mathfrak{R} \equiv 0\,(\overline{\mathfrak{R}}); \qquad \overline{\mathfrak{R}} \equiv 0\,(\mathfrak{R}); \qquad \mathfrak{R} = \overline{\mathfrak{R}};$$

isolierte Ideale sind also *eindeutig* durch die zugehörigen Primideale bestimmt. Dies ergibt insbesondere eine Verschärfung der Sätze VII und IX über die Zerlegung in irreduzible bzw. größte primäre Ideale, wobei nach dem Zusatz zu Satz IX nur kürzeste Darstellung vorausgesetzt zu werden braucht. Zusammenfassend kommt:

Satz XIII. *Bei jeder kürzesten Darstellung eines Ideals als kleinstes gemeinsames Vielfaches von irreduziblen bzw. größten primären Idealen sind die isolierten irreduziblen bzw. größten primären Ideale eindeutig bestimmt; die Vieldeutigkeit bezieht sich nur auf die nicht-isolierten irreduziblen bzw. größten primären Ideale*[31]). *Allgemein sind die isolierten Ideale eindeutig durch die zugehörigen Primideale bestimmt.*

Sind in einer solchen kürzesten Darstellung durch irreduzible, bzw. größte primäre Ideale die Ideale $\mathfrak{B}_i$ bzw. $\mathfrak{D}_j$ nicht-isoliert, so sind nach Definition die Komplemente $\mathfrak{A}_i$ bzw. $\mathfrak{Q}_j$ durch $\mathfrak{P}_i$ bzw. $\mathfrak{P}_j$ teilbar. Es kommt also

$$\mathfrak{A}_i^{\varrho_i} \equiv 0\,(\mathfrak{B}_i) \quad \text{bzw.} \quad \mathfrak{Q}_j^{\sigma_j} \equiv 0\,(\mathfrak{D}_j).$$

Aus dem Erfülltsein dieser Relationen folgt umgekehrt, daß $\mathfrak{P}_i$ bzw. $\mathfrak{P}_j$ in mindestens einem zugehörigen Primideal des Komplements, also nach

---

[30]) Würde man gewöhnliche zugehörige Primideale (§ 5 Schluß) einführen, so wäre als besondere Bedingung zuzufügen, daß diejenigen von $\mathfrak{Q}$ alle von denen von $\mathfrak{R}$ verschieden sind. Nach der Definition VI a braucht also die Darstellung nicht mehr reduziert in bezug auf das Komplement vorausgesetzt zu werden.

[31]) Dieser Satz ist für Ideale aus Polynomen im Fall der Zerlegung in größte primäre schon ohne Beweis von Macaulay mitgeteilt; seine Definition der isolierten und nicht-isolierten (imbedded) primären Ideale kann als irrationale Fassung der unten mitgeteilten angesehen werden.

Zusatz zu Satz IX auch in einem zugehörigen Primideal des eine reduzierte Darstellung in bezug auf $\mathfrak{Q}_j^*$ vermittelnden Teilers $\mathfrak{Q}_j^*$ von $\mathfrak{Q}_j$, aufgeht; $\mathfrak{B}_i$ bzw. $\mathfrak{Q}_j$ sind also nicht-isoliert. Insbesondere sind irreduzible Ideale $\mathfrak{B}_i$, deren zugehöriges Primideal öfter als einmal bei der Zerlegung von $\mathfrak{M}$ auftritt, stets nicht-isoliert. *Nicht-isolierte primäre Ideale sind also auch dadurch charakterisiert, daß eine Potenz jedes Komplements durch sie teilbar wird; isolierte primäre dadurch, daß dies nicht erfüllt sein kann.*

§ 8.

Eindeutige Darstellung eines Ideals als Produkt von teilerfremd-irreduziblen Idealen.

Besitzt der zugrunde gelegte Ringbereich Σ eine Einheit, d. h. ein Element ε, derart, daß $\varepsilon \cdot a = a$ wird für jedes Element aus Σ[32]), so lassen sich die teilerfremden Ideale definieren durch

Definition VIII. *Zwei Ideale $\mathfrak{R}$ und $\mathfrak{S}$ heißen teilerfremd, wenn ihr größter gemeinsamer Teiler gleich dem aus allen Elementen von Σ bestehenden Einheitsideal $\mathfrak{O} = (\varepsilon)$ ist. Ein Ideal heißt teilerfremd-irreduzibel, wenn es sich nicht als kleinstes gemeinsames Vielfaches von paarweise teilerfremden Idealen darstellen läßt.*

Es sei bemerkt, daß zwei teilerfremde Ideale immer gegenseitig relativprim sind. Nach Definition gibt es nämlich zwei Elemente: $r \equiv 0\,(\mathfrak{R})$, $s \equiv 0\,(\mathfrak{S})$ derart, daß $\varepsilon = r + s$ wird. Aus $\mathfrak{T} \cdot \mathfrak{R} \equiv 0\,(\mathfrak{S})$ folgt aber: $\mathfrak{T} \cdot r \equiv 0\,(\mathfrak{S})$, also $\mathfrak{T} \cdot \varepsilon = \mathfrak{T} \equiv 0\,(\mathfrak{S})$; und entsprechend kommt aus $\overline{\mathfrak{T}} \cdot \mathfrak{S} \equiv 0\,(\mathfrak{R})$ auch $\overline{\mathfrak{T}} \equiv 0\,(\mathfrak{R})$[33]). Aus Hilfssatz V folgt also, daß jede Darstellung durch paarweise teilerfremde Ideale zugleich *reduziert* ist.

Dem Eindeutigkeitsbeweise liegt zugrunde der Satz X entsprechende

Satz XIV. *Ist $\mathfrak{R}$ teilerfremd zu jedem der Ideale $\mathfrak{S}_1 \ldots \mathfrak{S}_\lambda$, so ist $\mathfrak{R}$ auch teilerfremd zu $\mathfrak{S} = [\mathfrak{S}_1 \ldots \mathfrak{S}_\lambda]$. Umgekehrt folgt aus der Teilerfremdheit von $\mathfrak{R}$ und $\mathfrak{S}$ auch die von $\mathfrak{R}$ mit jedem $\mathfrak{S}_j$. Ist $\mathfrak{R} = [\mathfrak{R}_1 \ldots \mathfrak{R}_\mu]$ und jedes $\mathfrak{R}_i$ teilerfremd zu jedem $\mathfrak{S}_j$, so sind $\mathfrak{R}$ und $\mathfrak{S}$ teilerfremd; auch hier gilt die Umkehrung.*

Ist nämlich $\mathfrak{R}$ teilerfremd zu jedem $\mathfrak{S}_j$, so existieren Elemente s_j, derart, daß

$$s_j \equiv 0\,(\mathfrak{S}_j); \qquad s_j \equiv \varepsilon\,(\mathfrak{R})$$

---

[32]) Σ kann bekanntlich wegen der Kommutativität der Multiplikation nicht mehr als *eine* Einheit besitzen, denn für irgend zwei Einheiten, ε_1 und ε_2, gilt: $\varepsilon_1 \varepsilon_2 = \varepsilon_2 = \varepsilon_1$.

[33]) Die Umkehrung gilt dagegen nicht; z. B. sind die Ideale $\mathfrak{R} = (x)$, $\mathfrak{S} = (y)$ gegenseitig relativprim, aber nicht teilerfremd.

wird. Folglich wird

$$s_1 \cdot s_2 \ldots s_\lambda \equiv 0\,(\mathfrak{S}); \qquad s_1 \cdot s_2 \ldots s_\lambda \equiv s\,(\mathfrak{R}), \qquad (\mathfrak{R}, \mathfrak{S}) = (s).$$

Da aber $(\mathfrak{R}, \mathfrak{S})$ durch jedes $(\mathfrak{R}, \mathfrak{S}_j)$ teilbar ist, gilt auch die Umkehrung. Die mehrfache Anwendung des Schlusses ergibt den zweiten Teil der Behauptung. Ist nämlich $\mathfrak{R}_i$ für festes i teilerfremd zu $\mathfrak{S}_1 \ldots \mathfrak{S}_\lambda$, so wird $\mathfrak{R}_i$ teilerfremd zu $\mathfrak{S}$. Gilt dies für jedes i, so wird, da der Begriff der Teilerfremdheit ein gegenseitiger ist, $\mathfrak{S}$ teilerfremd zu $\mathfrak{R}$. Umgekehrt folgt aus der Teilerfremdheit von $\mathfrak{R}$ und $\mathfrak{S}$ die Teilerfremdheit von $\mathfrak{S}$ zu $\mathfrak{R}_i$, und folglich von $\mathfrak{R}_i$ zu $\mathfrak{S}_j$.

Der Beweis für Existenz und Eindeutigkeit[34]) der Zerlegung in teilerfremd-irreduzible Ideale kommt, wie der entsprechende Beweis bei den relativprimen Idealen, auf eine *eindeutige* Gruppeneinteilung heraus. Da aber die relativprim-irreduziblen Ideale $\mathfrak{R}_1 \ldots \mathfrak{R}_\sigma$ von $\mathfrak{M}$ nach Satz XII *eindeutig* definiert sind, ist hier ein Zurückgehen auf die zugehörigen Primideale unnötig.

Wir fassen die eindeutig definierten relativprim-irreduziblen Ideale $\mathfrak{R}_1 \ldots \mathfrak{R}_\sigma$ von $\mathfrak{M}$ derart in Gruppen zusammen, daß *jedes Ideal einer Gruppe teilerfremd zu jedem Ideal einer davon verschiedenen Gruppe wird, während die einzelne Gruppe sich nicht in zwei Teilgruppen spalten läßt, derart daß jedes Ideal einer Teilgruppe teilerfremd zu jedem Ideal der andern Teilgruppe wird.* Eine solche Gruppeneinteilung ergibt sich wie folgt: Nach Definition muß die einzelne Gruppe G neben jedem Ideal $\mathfrak{R}$ auch alle zu $\mathfrak{R}$ nicht teilerfremden Ideale enthalten. Seien diese etwa gegeben durch $\mathfrak{R}_{i_1}$; zu diesen seien $\mathfrak{R}_{i_1 i_2}$ nicht teilerfremd; sei allgemein $\mathfrak{R}_{i_1 \ldots i_\lambda}$ nicht teilerfremd zu $\mathfrak{R}_{i_1 \ldots i_{\lambda-1}}$. Da es sich im ganzen nur um endlich viele Ideale handelt, muß das Verfahren nach endlich vielen Schritten abbrechen, d. h. keine von allen vorangehenden verschiedenen Ideale liefern; der so gewonnene Inbegriff von Idealen bildet eine Gruppe G von den gewünschten Eigenschaften. Denn alle nicht in G enthaltenen Ideale sind nach Konstruktion von G teilerfremd zu allen in G enthaltenen. Liegt ferner eine Einteilung in zwei Teilgruppen $G^{(1)}$ und $G^{(2)}$ vor; und sei etwa $\mathfrak{R}_{i_1 \ldots i_\lambda}$ Element von $G^{(1)}$. Da die Eigenschaft der Teilerfremdheit eine gegenseitige ist, muß $G^{(1)}$ dann auch $\mathfrak{R}_{i_1 \ldots i_{\lambda-1}}, \ldots \mathfrak{R}_{i_1}$, also auch $\mathfrak{R}$ und folglich die ganze Gruppe G enthalten, womit die Irreduzibilität bewiesen ist. Verfährt man mit den nicht in G enthaltenen Gruppen

---

[34]) Die Existenz der Zerlegung läßt sich wieder in Analogie zu § 2 direkt beweisen; auch der Eindeutigkeitsbeweis läßt sich direkt führen (vgl. das in der Einleitung über Schmeidler und Noether-Schmeidler Gesagte). Der hier gegebene Beweis gibt zugleich Einblick in die Struktur der teilerfremd-irreduziblen Ideale.

entsprechend, so kommt somit eine Gruppeneinteilung $G_1 \dots G_\tau$ aller $\mathfrak{R}$. Diese Gruppeneinteilung ist *eindeutig*; denn sei $G_1' \dots G_{\tau'}'$ eine zweite Einteilung und $\mathfrak{R}_{i_1 \dots i_\lambda}$ ein Element von G_i'. Dann enthält G_i' auch $\mathfrak{R}$ und folglich G_1 und kann wegen der Irreduzibilitätsbedingung keine von G_1 verschiedenen Elemente enthalten; es wird G_i' gleich G_1.

Es sei jetzt $\mathfrak{T}_i$ das kleinste gemeinsame Vielfache der in einer Gruppe G_i vereinigten Ideale $\mathfrak{R}$. Wir zeigen, daß $\mathfrak{M} = [\mathfrak{T}_1 \dots \mathfrak{T}_\tau]$ *eine Darstellung von* $\mathfrak{M}$ *durch teilerfremd-irreduzible Ideale wird.* Vorerst zeigt die Auflösung der $\mathfrak{T}$ in die $\mathfrak{R}$, daß $[\mathfrak{T}_1 \dots \mathfrak{T}_\tau]$ wirklich $\mathfrak{M}$ darstellt. Nach Satz XIV sind ferner die $\mathfrak{T}$ paarweise teilerfremd, und jedes $\mathfrak{T}$ ist teilerfremd-irreduzibel. Damit ist also die *Existenz* einer solchen Darstellung bewiesen.

Zum Eindeutigkeitsbeweis sei $\mathfrak{M} = [\overline{\mathfrak{T}}_1 \dots \overline{\mathfrak{T}}_{\bar\tau}]$ eine zweite derartige Darstellung. Löst man die $\overline{\mathfrak{T}}$ in ihre relativprim-irreduziblen Ideale $\mathfrak{R}$ auf, so sind die bei verschiedenen $\overline{\mathfrak{T}}$ auftretenden $\mathfrak{R}$ nach Satz XIV zueinander teilerfremd, also auch gegenseitig relativprim; sie stimmen also mit den eindeutig definierten relativprim-irreduziblen Idealen $\mathfrak{R}$ von $\mathfrak{M}$ überein. Die $\overline{\mathfrak{T}}_i$ erzeugen ferner nach Satz XIV eine Gruppeneinteilung G_i' der $\mathfrak{R}$ mit den angegebenen Eigenschaften. Da aber diese Gruppeneinteilung *eindeutig* ist und jedes $\overline{\mathfrak{T}}_i$ durch die Gruppe $G_i' = G_i$ *eindeutig* bestimmt ist, wird $\overline{\mathfrak{T}}_i = \mathfrak{T}_i$, womit die *Eindeutigkeit bewiesen* ist.

Für paarweise teilerfremde Ideale wird ferner das *kleinste gemeinsame Vielfache gleich dem Produkt.*

Denn nach Satz XIV ist für $\mathfrak{M} = [\mathfrak{T}_1 \dots \mathfrak{T}_\tau]$ auch das Komplement $\mathfrak{L}_i$ teilerfremd zu $\mathfrak{T}_i$; es gibt also Elemente

$$t_i \equiv 0\,(\mathfrak{T}_i); \qquad l_i \equiv 0\,(\mathfrak{L}_i); \qquad \varepsilon = t_i + l_i.$$

Aus $f \equiv 0\,(\mathfrak{T}_i)$; $f \equiv 0\,(\mathfrak{L}_i)$ folgt also wegen

$$f = f\varepsilon = ft_i + fl_i \quad \text{auch} \quad f \equiv 0\,(\mathfrak{L}_i \cdot \mathfrak{T}_i).$$

Da umgekehrt $\mathfrak{L}_i \cdot \mathfrak{T}_i$ durch $[\mathfrak{L}_i, \mathfrak{T}_i]$ teilbar, kommt $[\mathfrak{L}_i, \mathfrak{T}_i] = \mathfrak{L}_i \cdot \mathfrak{T}_i$; und durch Fortsetzung des Verfahrens auf $\mathfrak{L}_i$ schließlich:

$$\mathfrak{M} = [\mathfrak{T}_1 \dots \mathfrak{T}_\tau] = \mathfrak{T}_1 \cdot \mathfrak{T}_2 \cdot \dots \cdot \mathfrak{T}_\tau.$$

Damit ist bewiesen:

Satz XV. *Jedes Ideal läßt sich eindeutig darstellen als Produkt von endlich vielen paarweise teilerfremden und teilerfremd-irreduziblen Idealen.*

§ 9.

Ausdehnung der Untersuchung auf Moduln. Anzahlgleichheit der Komponenten bei Zerlegungen in irreduzible Moduln.

Wir zeigen jetzt, daß der Inhalt der drei ersten Paragraphen, der sich auf *irreduzible*, nicht auf primäre und Prim-Ideale bezieht, unter geringeren Voraussetzungen bestehen bleibt. Diese Paragraphen benutzen nämlich das kommutative Gesetz der Multiplikation nicht und beziehen sich nur auf die Eigenschaft der Ideale, Moduln zu sein, bleiben also erhalten für Moduln in bezug auf nicht-kommutative Bereiche, die jetzt zu definieren sind. Der Definition der Moduln ist ein *Doppelbereich* (Σ, T) zugrunde zu legen von folgenden Eigenschaften:

Σ *ist ein abstrakt-definierter nicht-kommutativer Ring*, d. h. Σ ist ein System von Elementen $a, b, c, \ldots$, für die zwei Verknüpfungsarten definiert sind, die Ringaddition $(\#)$ und die Ringmultiplikation $(\times)$, die den in § 1 aufgestellten Gesetzen genügen, mit Ausnahme des kommutativen Gesetzes 4. der Ringmultiplikation.

T ist ein System von Elementen $\alpha, \beta, \gamma, \ldots$, für das in Verbindung mit Σ ebenfalls zwei Verknüpfungen definiert sind, die *Addition*, die aus je zwei Elementen α, β eindeutig ein drittes $\alpha + \beta$ erzeugt; die *Multiplikation eines Elementes* α *aus* T *mit einem Element* c *aus* Σ, die eindeutig ein Element $c \cdot \alpha$ aus T erzeugt[35]).

Für diese Verknüpfungen gelten die folgenden Gesetze:

1. Das assoziative Gesetz der Addition: $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$.
2. Das kommutative Gesetz der Addition: $\alpha + \beta = \beta + \alpha$.
3. Das Gesetz der unbeschränkten und eindeutigen Subtraktion: es gibt in T ein und nur ein Element ξ, das die Gleichung $\alpha + \xi = \beta$ befriedigt (man bezeichnet $\xi = \beta - \alpha$).
4. Das assoziative Gesetz der Multiplikation: $a \cdot (b \cdot \gamma) = (a \times b) \cdot \gamma$.
5. Das distributive Gesetz: $(a \# b) \cdot \gamma = a \cdot \gamma + b \cdot \gamma$; $c \cdot (\alpha + \beta) = c \cdot \alpha + c \cdot \beta$.

Aus diesen Bedingungen folgt bekanntlich die Existenz des Nullelements, und die Gültigkeit des distributiven Gesetzes auch für die Verknüpfung von Subtraktion und Multiplikation:

$$(a \dot{-} b) \cdot \gamma = a \cdot \gamma - b \cdot \gamma; \qquad c \cdot (\alpha \dot{-} \beta) = c \cdot \alpha - c \cdot \beta;$$

wo $(\dot{-})$ die Subtraktion in Σ bedeutet. Enthält Σ eine Einheit ε, so soll $\varepsilon \cdot \alpha = \alpha$ gelten für jedes Element α aus T.

---

[35]) Es handelt sich also hier um eine „rechtsseitige" Multiplikation, einen „rechtsseitigen" Bereich T und folglich um „rechtsseitige" Moduln und Ideale. Würde man für T eine linksseitige Multiplikation $\alpha \cdot c$ zugrunde legen, so käme eine entsprechende Theorie der linksseitigen Moduln und Ideale; M enthält neben α auch $\alpha \cdot c$. Das assoziative Gesetz wäre hier von der Form $(\gamma \cdot b) \cdot a = \gamma \cdot (b \times a)$.

Unter einem *Modul M* in (Σ, T) sei ein System von Elementen aus T verstanden, das den beiden Bedingungen genügt:

1. *M enthält neben* α *auch* $c \cdot \alpha$, *wo* c *ein beliebiges Element aus* Σ *ist.*
2. *M enthält neben* α *und* β *auch die Differenz* $\alpha - \beta$; also neben α auch $n\alpha$ für jede ganze Zahl n[36]).

Nach dieser Definition *bildet T selbst einen Modul in* (Σ, T). Fällt insbesondere der Bereich T und die dort festgelegten Verknüpfungen mit dem Bereich Σ und den dort geltenden Verknüpfungen zusammen, so geht der Modul M über in ein (rechtsseitiges) Ideal $\mathfrak{M}$ in Σ. Wird Σ noch als kommutativ angenommen, so entsteht der gewöhnliche Idealbegriff, der sich somit als Spezialfall des Modulbegriffs ergibt[37]).

Für Moduln bleiben alle Definitionen des § 1 erhalten: So bedeutet $\alpha \equiv 0\,(M)$ bzw. $N \equiv 0\,(M)$, daß α bzw. jedes Element von N Element von M ist; anders ausgedrückt, α bzw. N ist durch M teilbar. M wird ein echter Teiler von N, wenn M von N verschiedene Elemente enthält; aus $N \equiv 0\,(M)$, $M \equiv 0\,(N)$ folgt $M = N$. Auch die Definition des größten gemeinsamen Teilers und des kleinsten gemeinsamen Vielfachen bleibt wörtlich erhalten. Enthält der Modul M insbesondere eine endliche Anzahl von Elementen $\alpha_1 \ldots \alpha_\varrho$, derart, daß $M = (\alpha_1 \ldots \alpha_\varrho)$, d. h. $\alpha = c_1\alpha_1 + \ldots + c_\varrho\alpha_\varrho + n_1\alpha_1 + \ldots + n_\varrho\alpha_\varrho$ wird für jedes $\alpha \equiv 0\,(M)$, wobei die c_i Größen aus Σ, die n_i ganze Zahlen sind, so heißt M ein *endlicher Modul*, $\alpha_1 \ldots \alpha_\varrho$ eine *Modulbasis.*

Wir legen nun im folgenden, analog wie in § 1, nur *solche Bereiche* (Σ, T) *zugrunde, die die Endlichkeitsbedingung erfüllen*: *Jeder Modul in* (Σ, T) *ist ein endlicher, besitzt also eine Modulbasis.*

Dann gilt für diesen Bereich (Σ, T) Satz I von der endlichen Kette auch für Moduln, wie der dortige Beweis zeigt, und damit sind alle Voraussetzungen für die §§ 2 und 3 erfüllt. Es läßt sich Definition I und Hilfssatz I über kürzeste und reduzierte Darstellung direkt übertragen; ebenso

---

[36]) Die ganzen Zahlen sind wieder als abkürzende Zeichen, nicht als Ringelemente zu betrachten.

[37]) Das einfachste Beispiel eines Moduls bildet der Modul aus ganzzahligen Linearformen; Σ besteht hier aus allen ganzen rationalen Zahlen, T aus allen ganzzahligen Linearformen. Ein etwas allgemeinerer Modul entsteht, wenn man in Σ und T ganze algebraische Zahlen statt der ganzrationalen Zahlen nimmt, oder etwa alle geraden Zahlen. Betrachtet man statt der Linearformen jeweils den Komplex aller Koeffizienten als *ein* Element, so sind die Verknüpfungen in Σ und T tatsächlich verschiedene. Ideale in nicht-kommutativen Ringbereichen aus Polynomen bilden den Gegenstand der gemeinsamen Arbeit Noether-Schmeidler. Von Idealen in weiteren speziellen nichtkommutativen Bereichen handeln die Vorlesungen über die Zahlentheorie der Quaternionen von Hurwitz (Berlin, Springer 1919) und die dort zitierten Arbeiten von Du Pasquier.

Satz II über die Darstellbarkeit jedes Moduls als kleinstes gemeinsames Vielfaches von endlich vielen irreduziblen Moduln, wobei Hilfssatz II zeigt, daß jede solche kürzeste Darstellung zugleich reduziert ist. Weiter bleibt Satz III erhalten, der die Reduzibilität eines Moduls durch Eigenschaften seines Komplements ausdrückt; und daraus folgt Hilfssatz III und schließlich Satz IV, der die *Anzahlgleichheit der Komponenten bei zwei verschiedenen kürzesten Darstellungen eines Moduls als kleinstes gemeinsames Vielfaches von irreduziblen Moduln* aussagt. Satz IV ergibt noch den Hilfssatz IV als Umkehrung von Hilfssatz I über reduzierte Darstellung.

Zusatz. Dieselbe Überlegung zeigt, daß alle diese Sätze und Definitionen erhalten bleiben, wenn man für zweiseitige Bereiche T, d. h. solche, die sowohl rechts- wie linksseitig sind, unter Modul durchweg einen *zweiseitigen Modul* versteht, d. h. einen solchen, der neben α auch $c \cdot \alpha$ und $\alpha \cdot c$ enthält; neben α und β auch $\alpha - \beta$.

Während all diese Sätze sich nur auf den Begriff der *Teilbarkeit* und des *kleinsten gemeinsamen Vielfachen* stützen, beruhen die weiteren Eindeutigkeitssätze wesentlich auf dem *Produktbegriff* und lassen deshalb eine direkte Übertragung nicht zu. So läßt sich die Definition des primären und Prim-Ideals nicht auf Moduln übertragen, da das Produkt zweier Größen aus T nicht definiert ist. Die formal mögliche Übertragung auf nicht-kommutative Ringe verliert aber ihren Sinn, da hier die Existenz des zugehörigen Primideals sich nicht beweisen läßt[38]) und auch der Beweis, daß ein irreduzibles Ideal primär ist, versagt. Diese beiden Tatsachen bilden aber die Grundlage der folgenden Eindeutigkeitssätze. — Dagegen lassen sich, wenn der nichtkommutative Ring eine Einheit besitzt, die teilerfremden und teilerfremd-irreduziblen Ideale definieren, und die zum Beweise von Satz II benutzten Überlegungen lassen erkennen, daß jedes Ideal sich als kleinstes gemeinsames Vielfaches von *endlich vielen* paarweise teilerfremden und teilerfremd-irreduziblen Idealen darstellen läßt[39]).

Schließlich sei noch ein hinreichendes Kriterium dafür erwähnt, daß in (Σ, T) die Endlichkeitsbedingung erfüllt ist: *Enthält Σ eine Einheit*

---

[38]) Es folgt nämlich aus

$$p_1^{\lambda_1} \equiv 0\,(\mathfrak{Q}); \qquad p_2^{\lambda_2} \equiv 0\,(\mathfrak{Q}) \quad \text{hier nicht:} \quad (p_1 - p_2)^{\lambda_1+\lambda_2} \equiv 0\,(\mathfrak{Q})$$

und ebenso folgt aus

$$(a \cdot b)^{\lambda} \equiv 0\,(\mathfrak{Q}) \quad \text{nicht:} \quad a^{\lambda} \cdot b^{\lambda} \equiv 0\,(\mathfrak{Q}).$$

Dadurch läßt sich also $\mathfrak{P}$ weder als Ideal nachweisen, noch kommt ihm die Eigenschaft der Primideale zu. — Für zweiseitige Ideale läßt $\mathfrak{P}$ sich zwar als Ideal, nicht aber als Primideal nachweisen.

[39]) Für spezielle, „vollständig reduzible" Ideale lassen sich auch hier Eindeutigkeitssätze aufstellen; vgl. gemeinsame Arbeit Noether-Schmeidler.

und erfüllt die Endlichkeitsbedingung, und ist T selbst ein endlicher Modul in (Σ, T), so ist jeder Modul in (Σ, T) ein endlicher.

Aus der Existenz der Einheit in Σ folgt nämlich für

$$\mathfrak{M} = (f_1 \ldots f_\varrho); \qquad f = \bar{b}_1 f_1 + \ldots + \bar{b}_\varrho f_\varrho + n_1 f_1 + \ldots + n_\varrho f_\varrho,$$

wo $\bar{b}_i$ Elemente aus Σ, n_i ganze Zahlen sind, auch eine Darstellung: $f = b_1 f_1 + \ldots + b_\varrho f_\varrho$, wo b_i Elemente aus Σ sind. Denn wegen $f_i = \varepsilon f_i$ wird $n_i f_i = n_i \varepsilon f_i$, und da $n_i \varepsilon = (\varepsilon + \ldots + \varepsilon)$ zu Σ gehört, wird $b_i = \bar{b}_i + n_i \varepsilon$ ein Element aus Σ. Die Voraussetzung über T sagt nun aus, daß jedes Element α aus T eine Darstellung zuläßt:

$$\alpha = \bar{a}_1 \tau_1 + \ldots + \bar{a}_k \tau_k + n_1 \tau_1 + \ldots + n_k \tau_k,$$

und folglich:

$$\alpha = a_1 \tau_1 + \ldots + a_k \tau_k,$$

wo die zweite Darstellung wegen $\varepsilon \tau_i = \tau_i$ sich wie oben aus der ersten ergibt.

Durchlaufen nun die α die Elemente eines Moduls M aus (Σ, T), so durchlaufen die Koeffizienten a_k von τ_k ein Ideal $\mathfrak{M}_k$ aus Σ; nach dem Obigen wird also für jedes $a_k \equiv 0\ (\mathfrak{M}_k)$ auch $a_k = b_1 a_k^{(1)} + \ldots + b_\varrho a_k^{(\varrho)}$. Bezeichnet $\alpha^{(i)}$ ein Element aus M, für das der Koeffizient von τ_k gleich $a_k^{(i)}$ wird, so wird $\alpha - b_1 \alpha^{(1)} \ldots - b_\varrho \alpha^{(\varrho)}$ ein zu M gehöriges Element, das nur von $\tau_1, \ldots, \tau_{k-1}$ abhängt. Auf die Gesamtheit dieser τ_k nicht mehr enthaltenden Elemente, die einen Modul M' bilden, läßt sich das Verfahren wiederholen, so daß durch endlich oftmalige Wiederholung die *Behauptung bewiesen* ist.

§ 10.

Spezialfall des Polynombereichs.

1. Der zugrunde gelegte Ringbereich Σ bestehe aus allen Polynomen von $x_1 \ldots x_n$ mit beliebigen komplexen Koeffizienten, für den nach dem Hilbertschen Theorem von der Modulbasis (Ann. 36) die Endlichkeitsbedingung erfüllt ist. Es handelt sich um den *Zusammenhang unserer Sätze mit den bekannten Sätzen der Eliminations- und Modultheorie.*

Dieser Zusammenhang wird hergestellt durch den folgenden Spezialfall eines bekannten Hilbertschen Satzes[40]):

Verschwindet f für jedes (endliche) Wertsystem von $x_1 \ldots x_n$, das Nullstelle aller Polynome eines Primideals $\mathfrak{P}$ (Nullstelle von $\mathfrak{P}$) ist, so ist f durch $\mathfrak{P}$ teilbar. M. a. W.: Ein Primideal $\mathfrak{P}$ besteht aus der *Gesamtheit* der Polynome, die in seinen Nullstellen verschwinden[41]).

---

[40]) Über die vollen Invariantensysteme. Math. Ann. **42** (1893), § 3, S. 313.

[41]) Dieser Spezialfall läßt sich, wie Lasker [Math. Ann. **60** (1905), S. 607] gezeigt hat, im Fall homogener Formen auch direkt beweisen, und es folgt dann umgekehrt hieraus wieder der Hilbertsche Satz (im homogenen und inhomogenen Fall),

Verschwindet somit ein Produkt $f \cdot g$ für alle Nullstellen von $\mathfrak{P}$, so verschwindet mindestens ein Faktor; die Nullstellen bilden ein *irreduzibles algebraisches Gebilde*. Legt man umgekehrt diese Definition des irreduziblen Gebildes zugrunde, so zeigt sich, daß die Gesamtheit der in einem irreduziblen Gebilde verschwindenden Polynome ein Primideal bilden; Primideal und irreduzibles Gebilde entsprechen sich somit eineindeutig. Wegen $\mathfrak{Q} \equiv 0\ (\mathfrak{P})$, $\mathfrak{P}^e \equiv 0\ (\mathfrak{Q})$ stimmen ferner die Nullstellen eines primären Ideals mit denen seines zugehörigen Primideals überein[42]). Die Darstellung eines Ideals als kleinstes gemeinsames Vielfaches von größten primären Idealen ergibt also eine Auflösung aller Nullstellen des Ideals in irreduzible Gebilde; und wie Lasker gezeigt hat, gilt auch das Umgekehrte. *Der Eindeutigkeitsnachweis der zugehörigen Primideale entspricht also hier dem Fundamentalsatz der Eliminationstheorie von der eindeutigen Zerlegbarkeit eines algebraischen Gebildes in irreduzible Gebilde;* kann für spezielle Polynombereiche, wo keine eindeutige Produktdarstellung der Polynome durch irreduzible Polynome des Bereichs und folglich auch keine Eliminationstheorie besteht, als Äquivalent dieses Satzes der Eliminationstheorie gelten.

Die den isolierten primären Idealen entsprechenden irreduziblen Gebilde sind genau die bei der „Minimalresolvente“[43]) auftretenden; denn die Nullstellen jedes nicht-isolierten größten primären Ideals sind zugleich Nullstellen mindestens eines isolierten; nämlich eines solchen, dessen zugehöriges Primideal durch das des nicht-isolierten Ideals teilbar ist. Die Eindeutigkeit der isolierten primären Ideale ergibt also in den Exponenten neue invariante Multiplizitätszahlen. Auch die Eindeutigkeitssätze bei der Auflösung der primären Ideale in irreduzible können als Ergänzung der Eliminationstheorie im Sinn der Multiplizität angesehen werden.

---

den wir so aussprechen können: Verschwindet ein Ideal $\mathfrak{R}$ in allen Nullstellen von $\mathfrak{M}$, so ist eine Potenz von $\mathfrak{R}$ durch $\mathfrak{M}$ teilbar. Dieser Satz, und ebenso der Spezialfall, gilt aber nur, wenn der Wertevorrat der x *algebraisch abgeschlossen* ist, kann daher aus unsern Sätzen allein nicht folgen, sondern muß die Wurzelexistenz benutzen; etwa an der Stelle, daß ein Ideal, dessen Nullstellen nur aus $x_1 = 0 \ldots x_n = 0$ bestehen, alle Potenzprodukte der x von einer gewissen Dimension an enthält. Der übrige Beweis läßt sich unter Benutzung unserer Sätze gegenüber Lasker etwas vereinfachen. Lasker muß nämlich auch zum Nachweis der Zerlegung eines Ideals in größte primäre den Hilbertschen Satz heranziehen.

[42]) Diese Eigenschaft eines primären Ideals, ein irreduzibles Gebilde zu besitzen, nimmt Macaulay (vgl. Einleitung) zur Definition, während Lasker nur den Begriff der Mannigfaltigkeit eines Gebildes in die Definition aufnimmt, im übrigen abstrakt definiert. Die nur für $x_1 = 0 \ldots x_n = 0$ verschwindenden primären Ideale nehmen bei Lasker eine Sonderstellung ein.

[43]) Vgl. etwa J. König, Einleitung in die allgemeine Theorie der algebraischen Größen (Leipzig, Teubner, 1903), S. 235.

Nach diesen Bemerkungen lassen sich die verschiedenen Zerlegungen in ihrem Verhalten zu den algebraischen Gebilden deuten. Den paarweise teilerfremden Idealen entsprechen solche Gebilde, die keine gemeinsame Nullstelle besitzen; bei den gegenseitig relativprimen Idealen ist kein irreduzibles Gebilde des einen Ideals zugleich gemeinsame Nullstelle; die größten primären Ideale verschwinden nur in irreduzibeln Gebilden, die alle voneinander verschieden sind; bei der Zerlegung in irreduzible Ideale können dieselben irreduziblen Gebilde auch mehrfach auftreten.

Bemerkt sei noch, daß an Stelle des allgemeinen Polynombereichs auch der Bereich aller homogenen Formen zugrunde gelegt werden kann, denn man überzeugt sich leicht, daß auch bei den dort geltenden Verknüpfungen — die Addition ist nur für Formen gleicher Dimensionen definiert — die allgemeinen Sätze erhalten bleiben[44]).

Ein einfachstes Beispiel der vier verschiedenen Zerlegungen — für das die Formeln unten folgen — ist nach dem obigen etwa gegeben durch eine Gerade und zwei dazu windschiefe, sich schneidende Gerade, von denen eine einen vom Schnittpunkt verschiedenen Punkt in höherer Multiplizität enthält. Der Zerlegung in teilerfremd-irreduzible Ideale entspricht die Zerlegung in die Gerade und das dazu windschiefe Gebilde; dies Gebilde zerfällt bei der Zerlegung in relativprim-irreduzible Ideale in die beiden Geraden; der Zerlegung in größte primäre Ideale entspricht eine Ablösung des Punktes höherer Multiplizität, während die Zerlegung in irreduzible Ideale eine Auflösung dieses Punktes bedingt.

Nimmt man diesen Punkt zum Anfangspunkt, die durchlaufende Gerade zur y-Achse, die diese schneidende Gerade der x-Achse parallel, die dazu windschiefe Gerade der z-Achse parallel, so wird eine solche Konfiguration etwa dargestellt durch die folgenden *irreduziblen Ideale*[45]):

$$\mathfrak{B}_1 = (x-1, y); \quad \mathfrak{B}_2 = (y-1, z); \quad \mathfrak{B}_3 = (x, z); \quad \mathfrak{B}_4 = (x^3, y, z);$$
$$\mathfrak{B}_5 = (x^2, y^2, z).$$

Die *zugehörigen Primideale* werden:

$$\mathfrak{P}_1 = \mathfrak{B}_1; \quad \mathfrak{P}_2 = \mathfrak{B}_2; \quad \mathfrak{P}_3 = \mathfrak{B}_3; \quad \mathfrak{P}_4 = \mathfrak{P}_5 = (x, y, z).$$

Die *größten primären Ideale* werden:

$$\mathfrak{Q}_1 = \mathfrak{B}_1; \quad \mathfrak{Q}_2 = \mathfrak{B}_2; \quad \mathfrak{Q}_3 = \mathfrak{B}_3; \quad \mathfrak{Q}_4 = [\mathfrak{B}_4, \mathfrak{B}_5] = (x^3, y^2, x^2 y, z).$$

Die *relativprim-irreduziblen Ideale* werden:

$$\mathfrak{R}_1 = \mathfrak{Q}_1; \quad \mathfrak{R}_2 = \mathfrak{Q}_2; \quad \mathfrak{R}_3 = [\mathfrak{Q}_3, \mathfrak{Q}_4] = (x^3, x^2 y, x y^2, z).$$

---

[44]) Daß hier aber im Falle der Mehrdeutigkeit neben homogenen auch inhomogene Zerlegungen existieren können, zeigt das Beispiel:

$$(x^3, xy, y^3) = [(x^3, y); (y^3, x)] = [(xy, x^3, y^3, x+y^3); (xy, x^3, y^3, y+x^2)].$$

[45]) Davon sind die drei ersten als Primideale irreduzibel; $\mathfrak{B}_4$ da es nur die Teiler (x^2, y, z) und (x, y, z) besitzt; $\mathfrak{B}_5$ da *jeder* Teiler das Polynom xy enthält.

Die *teilerfremd-irreduzibeln Ideale* werden:

$$\mathfrak{S}_1 = \mathfrak{R}_1; \qquad \mathfrak{S}_2 = [\mathfrak{R}_2, \mathfrak{R}_3] = ((y-1)x^3, (y-1)x^2y, (y-1)xy^2, z).$$

Daraus kommt das *Gesamtideal*:

$$\mathfrak{M} = [\mathfrak{S}_1, \mathfrak{S}_2] = \mathfrak{S}_1 \cdot \mathfrak{S}_2$$
$$= ((x-1)(y-1)x^3, (y-1)x^2y, (y-1)xy^2, (x-1)z, y(y-1)x^3, yz),$$

wobei $$1 = -(y-1)x^3 + (y-1)(x^3-1) + y,$$

$$(y-1)(x^3-1) + y \equiv 0 \,(\mathfrak{S}_1); \qquad -(y-1)x^3 \equiv 0 \,(\mathfrak{S}_2).$$

Dabei sind die Ideale $\mathfrak{B}_1, \mathfrak{B}_2, \mathfrak{B}_3$ isolierte, also auch bei den Zerlegungen in irreduzible und größte primäre Ideale eindeutig bestimmt. Die Ideale $\mathfrak{B}_4$ und $\mathfrak{B}_5$ bzw. $\mathfrak{Q}_4$ sind nicht-isolierte; sie sind nicht eindeutig bestimmt, sondern etwa ersetzbar durch $\mathfrak{D}_4 = (x^3, y + \lambda x^2, z)$, $\mathfrak{D}_5 = (x^2 + \mu xy, y^2, z)$; ebenso ist $\mathfrak{Q}_4$ ersetzbar durch

$$\overline{\mathfrak{Q}}_4 = (x^3, x^2y, y^2 + \lambda xy, z).$$

2. Ebenso wie der allgemeine (und der ganzzahlige) Polynombereich erfüllt auch jeder *endliche Integritätsbereich aus Polynomen* — wie das Hilbertsche Theorem von der Modulbasis zeigt — die Endlichkeitsbedingung[46]), wobei die Koeffizienten einem beliebigen Körper zugewiesen werden können. Wir geben noch ein Beispiel für den *Bereich aller geraden Polynome*, als dem einfachsten Bereich, wo wegen $x^2 \cdot y^2 = (xy)^2$ keine eindeutige Produktdarstellung der Polynome durch irreduzible Polynome des Bereichs existiert. Es handelt sich um die gleiche Konfiguration wie in dem obigen Beispiel, die jetzt gegeben wird durch die *irreduziblen Ideale*:

$$\mathfrak{B}_1 = (x^2-1, xy, y^2, yz); \qquad \mathfrak{B}_2 = (y^2-1, xz, yz, z^2);$$
$$\mathfrak{B}_3 = (x^2, xy, xz, yz, z^2); \qquad \mathfrak{B}_4 = (x^4, xy, y^2, xz, yz, z^2);$$
$$\mathfrak{B}_5 = (x^2, y^2, xz, yz, z^2).$$

Die *zugehörigen Primideale* werden:

$$\mathfrak{P}_1 = \mathfrak{B}_1; \quad \mathfrak{P}_2 = \mathfrak{B}_2; \quad \mathfrak{P}_3 = \mathfrak{B}_3; \quad \mathfrak{P}_4 = \mathfrak{P}_5 = (x^2, xy, y^2, xz, yz, z^2).$$

Daß $\mathfrak{P}_1$ Primideal wird, folgt daraus, daß jedes Polynom des Bereichs von der Form wird:

$$f \equiv \varphi(z^2) + xz\psi(z^2) \,(\mathfrak{P}_1).$$

Sei also

$$f_1 \equiv \varphi_1(z^2) + xz\psi_1(z^2); \qquad f_2 \equiv \varphi_2(z^2) + xz\psi_2(z^2),$$

[46]) Ist umgekehrt für einen Polynombereich die Endlichkeitsbedingung erfüllt, und läßt jedes Polynom mindestens eine Darstellung zu, wo die Multiplikatoren von geringerem Grad in x sind, so ist der Bereich ein endlicher Integritätsbereich.

so folgt aus $f_1 \cdot f_2 \equiv 0 (\mathfrak{P}_1)$ das Bestehen der Gleichungen:

$$\varphi_1 \varphi_2 + z^2 \psi_1 \psi_2 = 0; \qquad \varphi_2 \psi_1 + \varphi_1 \psi_2 = 0$$

und daraus $f_1 \equiv 0 (\mathfrak{P}_1)$ oder $f_2 \equiv 0 (\mathfrak{P}_1)$.

Genau so zeigt sich, daß $\mathfrak{P}_2$ Primideal wird; $\mathfrak{P}_3$ wird Primideal, da jedes Polynom des Bereichs mod $\mathfrak{P}_3$ einem Polynom von y^2 kongruent wird; $\mathfrak{P}_4$ besteht aus allen Polynomen des Bereichs. Es werden also auch $\mathfrak{B}_1$; $\mathfrak{B}_2$ und $\mathfrak{B}_3$ als Primideale irreduzibel; $\mathfrak{B}_4$ und $\mathfrak{B}_5$ besitzen aber je nur den einzigen echten Teiler $\mathfrak{P}_4$, sind also notwendig irreduzibel.

Aus den irreduziblen Idealen ergeben sich die *größten primären*:

$$\mathfrak{Q}_1 = \mathfrak{B}_1; \quad \mathfrak{Q}_2 = \mathfrak{B}_2; \quad \mathfrak{Q}_3 = \mathfrak{B}_3; \quad \mathfrak{Q}_4 = [\mathfrak{B}_4, \mathfrak{B}_5] = (x^4, x^3 y, y^2, xz, yz, z^2);$$

die *relativprim-irreduziblen Ideale*:

$$\mathfrak{R}_1 = \mathfrak{Q}_1; \quad \mathfrak{R}_2 = \mathfrak{Q}_2; \quad \mathfrak{R}_3 = [\mathfrak{Q}_3, \mathfrak{Q}_4] = (x^4, x^3 y, x^2 y^2, xy^3, xz, yz, z^2),$$

die *teilerfremd-irreduziblen Ideale*:

$$\mathfrak{S}_1 = \mathfrak{R}_1; \qquad \mathfrak{S}_2 = [\mathfrak{R}_2, \mathfrak{R}_3]$$
$$= ((y^2-1)x^4, (y^2-1)x^3 y, (y^2-1)x^2 y^2, (y^2-1)xy^3, xz, yz, z^2).$$

Es wird wie im ersten Beispiel:

$$[\mathfrak{B}_4, \mathfrak{B}_5] = [\mathfrak{D}_4, \mathfrak{D}_5];$$

wo $\mathfrak{D}_4 = (x^4, xy + \lambda x^2, \ldots); \quad \mathfrak{D}_5 = (x^2 + \mu xy, \ldots) \quad \lambda \cdot \mu \neq 1;$

$$[\mathfrak{Q}_3, \mathfrak{Q}_4] = [\mathfrak{Q}_3, \overline{\mathfrak{Q}}_4]; \quad \text{wo} \quad \overline{\mathfrak{Q}}_4 = (x^4, x^3 y, y^2 + \lambda xy, \ldots).$$

Die übrigen irreduziblen bzw. größten primären Ideale $\mathfrak{B}_1$, $\mathfrak{B}_2$, $\mathfrak{B}_3$ sind als isolierte Ideale eindeutig bestimmt.

§ 11.

Beispiele aus der Zahlentheorie und der Theorie der Differentialausdrücke.

1. Der zugrunde gelegte Bereich Σ bestehe aus allen *geraden, ganzen rationalen Zahlen.* Σ läßt sich also eineindeutig dem Bereich aller ganzen rationalen Zahlen zuordnen, indem man jeder Zahl $2a$ aus Σ die Zahl a entsprechen läßt. Daraus folgt sofort, daß jedes Ideal in Σ ein Hauptideal $(2a)$ ist, wobei in der Basisdarstellung $2c = n \cdot 2a$ für jedes Element $2c$ des Ideals die ungeraden n nur Abkürzungen für die endlichen Summen bedeuten.

Die *Primideale* des Bereichs sind gegeben durch $\mathfrak{P}_0 = \mathfrak{O} = (2)$ und $\mathfrak{P} = (2p)$, wo p eine ungerade Primzahl bedeutet; es ist also jedes Primideal durch $\mathfrak{P}_0$, aber durch kein weiteres Primideal teilbar. Die *primären Ideale* sind gegeben durch $\mathfrak{Q}_{\varrho_0} = (2 \cdot 2^{\varrho_0})$ und $\mathfrak{Q}_\varrho = (2p^\varrho)$; sie sind zugleich *irreduzible Ideale,* und nach dem über die Primideale Gesagten sind je zwei zu verschiedenen ungeraden Primzahlen gehörige gegen-

seitig relativprim, aber kein $\mathfrak{Q}$ ist zu irgendeinem $\mathfrak{Q}_{\varrho_0}$ relativprim[47]), die $\mathfrak{Q}_{\varrho_0}$ sind also die einzigen nicht-isolierten primären Ideale. Der eindeutigen Zerlegung von a in Primzahlpotenzen entspricht die *eindeutige* Darstellung des Ideals $(2a)$ durch größte primäre, zugleich irreduzible Ideale:

$$(2a) = [(2 \cdot 2^{\varrho_0}),\ (2p_1)^{\varrho_1},\ \ldots,\ (2p_a)^{\varrho_a}];$$

es sind also hier im Gegensatz zu den Beispielen aus dem Polynombereich auch die *nicht-isolierten* größten primären Ideale *eindeutig* bestimmt. Für $\varrho_0 = 0$ handelt es sich zugleich um eine Darstellung durch gegenseitig relativprime Ideale, während für $\varrho_0 > 0$ das Ideal relativprim-irreduzibel ist.

Während also im Bereich aller ganzen Zahlen die vier verschiedenen Zerlegungen zusammenfallen, ist dies hier nur der Fall für die beiden Zerlegungen in größte primäre und irreduzible einerseits, und bei $\varrho_0 > 0$ für teilerfremd-irreduzible (jedes Ideal ist teilerfremd-irreduzibel, da der Bereich keine Einheit besitzt) und relativprim-irreduzible andererseits, während bei $\varrho_0 = 0$ die teilerfremd-irreduziblen und relativprim-irreduziblen Zerlegungen voneinander verschieden werden. Zugleich bietet sich hier schon ein Beispiel dafür, daß ein Primideal durch ein anderes teilbar sein kann, ohne damit identisch zu sein; allgemeiner dafür, daß *aus der Teilbarkeit nicht die Produktdarstellung folgt.* Das letztere — eine Folge davon, daß der Bereich keine Einheit enthält — ist auch der Grund dafür, daß keine eindeutige Produktdarstellung der Zahlen des Bereichs durch irreduzible Zahlen des Bereichs existiert, obwohl jedes Ideal ein Hauptideal wird; die Einführung des kleinsten gemeinsamen Vielfachen erweist sich also hier als notwendig. Es sei noch bemerkt, daß die Verhältnisse genau die *gleichen* bleiben, wenn statt aller geraden Zahlen alle durch eine *feste Primzahl oder Primzahlpotenz teilbaren Zahlen* zugrunde gelegt werden.

Dagegen werden auch noch *irreduzible und primäre Ideale verschieden*, wenn Σ aus *allen durch eine zusammengesetzte Zahl* $g = \mathfrak{p}_1^{\sigma_1} \ldots \mathfrak{p}_\nu^{\sigma_\nu}$ *teilbaren Zahlen* besteht. Es wird wieder jedes Ideal ein Hauptideal $(g \cdot a)$, und die *Primideale* sind wieder gegeben durch $\mathfrak{P}_0 = \mathfrak{D} = (g)$; $\mathfrak{P} = (g \cdot p)$, wo p eine von den in g aufgehenden Primzahlen $\mathfrak{p}$ verschiedene Primzahl bedeutet. Dagegen sind die *irreduziblen Ideale* gegeben durch $\mathfrak{B}_{\lambda_i} = (g \cdot \mathfrak{p}_i^{\lambda_i})$; $\mathfrak{B}_\varrho = (g \cdot p^\varrho)$; die *primären Ideale* durch $\mathfrak{Q}_\varrho = \mathfrak{B}_\varrho$ und durch die von den irreduziblen verschiedenen $\mathfrak{Q}_{\lambda_1 \ldots \lambda_\nu} = (g \cdot \mathfrak{p}_1^{\lambda_1} \ldots \mathfrak{p}_\nu^{\lambda_\nu})$, wobei die $\mathfrak{B}_{\lambda_i}$ und $\mathfrak{Q}_{\lambda_1 \ldots \lambda_\nu}$ alle dasselbe zugehörige Primideal $\mathfrak{P}_0 = (g)$ besitzen. Auch hier besteht Eindeutigkeit der Zerlegung in irreduzible Ideale, und folglich

---

[47]) In der Tat folgt aus: $2b \cdot 2p_1^{\varrho_1} \equiv 0\,(2p_2^{\varrho_2})$ für ungerade $p_1 \neq p_2$ stets: $2b \equiv 0\,(2p_2^{\varrho_2})$; aus $2b \cdot 2p^\varrho \equiv 0\,(2 \cdot 2^{\varrho_0})$ aber nur $2b \equiv 2 \cdot 2^{\varrho_0 - 1}\,(2 \cdot 2^{\varrho_0})$.

auch für die Zerlegung in größte primäre Ideale, es sind also wieder auch die nicht-isolierten Ideale eindeutig bestimmt.

2. Ein Beispiel eines *nicht-kommutativen Ringbereichs* bietet die in der Arbeit Noether-Schmeidler behandelte Idealtheorie in nicht-kommutativen Polynombereichen. Es handelt sich insbesondere um „vollständig-reduzible" Ideale, d. h. solche, bei denen die Komponenten der Zerleguug paarweise teilerfremd sind und keine echten Teiler besitzen; die Komponenten sind also a fortiori irreduzibel. Es ergibt sich somit in Ergänzung der dort bewiesenen Isomorphie nach § 9 noch die *Anzahlgleichheit der Komponenten* bei zwei verschiedenen Zerlegungen. Damit ist für die als Spezialfall der Arbeit sich ergebende Zerlegung der Systeme partieller oder gewöhnlicher linearer Differentialausdrücke ein Resultat gewonnen, das selbst in dem bekannten Fall eines gewöhnlichen linearen Differentialausdrucks nicht bemerkt gewesen zu sein scheint.

Zugleich liefert das System T aller Restklassen eines festen Ideals $\mathfrak{M}$ zusammen mit dem nicht-kommutativen Polynombereich Σ einen Doppelbereich (Σ, T), wo T Moduleigenschaft in bezug auf Σ hat. Denn die Differenz zweier Restklassen ist wieder eine Restklasse, und ebenso das Produkt einer Restklasse mit einem beliebigen Polynom, während das Produkt zweier Restklassen nicht existiert (a. a. O. § 3). Die dort als „Untergruppen" bezeichneten Systeme von Restklassen bilden somit Beispiele von Moduln in Doppelbereichen (Σ, T), wo der zugrunde gelegte Ringbereich Σ nicht-kommutativ ist.

§ 12.

Beispiel aus der Elementarteilertheorie.

Es handelt sich um eine durch die allgemeinen Entwicklungen bedingte Auffassung der Elementarteilertheorie, die aber selbst als *bekannt* vorausgesetzt wird.

Sei Σ der Bereich aller ganzzahligen Matrizen aus n^2 Elementen, für die Addition und Multiplikation in dem für Matrizen gebräuchlichen Sinn definiert sei. Σ wird also ein *nicht-kommutativer Ringbereich*; die Ideale sind somit im allgemeinen einseitig, die zweiseitigen nur als Spezialfall darin enthalten [48]).

Wir zeigen zuerst, daß *jedes Ideal* ein *Hauptideal* wird. Dazu ordnen

[48]) Die Idealtheorie dieser Bereiche bildet den Gegenstand der Arbeiten von Du Pasquier: Zahlentheorie der Tettarionen, Dissertation Zürich, Vierteljahrsschr. d. Naturf. Ges. Zürich, **51** (1906). Zur Theorie der Tettarionenideale, ibid,, **52** (1907). Der Inhalt der zweiten Arbeit ist der Nachweis, daß jedes Ideal ein Hauptideal wird.

wir (bei rechtsseitigen Idealen) jeder Matrix $A = (a_{ik})$ einen Modul

$$\mathsf{A} = (a_{11}\xi_1 + \ldots + a_{1n}\xi_n, \ldots, a_{n1}\xi_1 + \ldots + a_{nn}\xi_n)$$

aus ganzzahligen Linearformen zu. Umgekehrt entspricht diesem Modul jede Matrix, die eine Basis von A liefert, also neben A auch UA, wo U unimodular ist. Allgemeiner entspricht dem Produkt PA ein Modul B, der Vielfaches von A wird. Eine einzelne Linearform aus A wird durch solche P gegeben, die nur eine von Null verschiedene Zeile enthalten.

Seien nun $A_1, A_2, \ldots, A_\nu, \ldots$ alle Elemente eines Ideals $\mathfrak{M}$; $\mathsf{A}_1, \mathsf{A}_2, \ldots, \mathsf{A}_\nu, \ldots$ die ihnen zugeordneten Moduln, A deren größter gemeinsamer Teiler und UA die allgemeinste, diesem Modul A zugeordnete Matrix. Jeder einzelnen Linearform aus A entspricht dann nach der Definition des größten gemeinsamen Teilers eine Matrix $P_1 A_{i_1} + \ldots + P_\sigma A_{i_\sigma}$, wo nach dem obigen die P nur eine von Null verschiedene Zeile besitzen. Daraus folgt, daß auch die einer Basis von A entsprechende Matrix A eine solche Darstellung, jetzt mit allgemeinem P, zuläßt und folglich ein Element aus $\mathfrak{M}$ wird. Da ferner jeder Modul A_i durch A teilbar ist, wird jede Matrix A_i durch A teilbar; *A und allgemein UA bildet eine Basis von $\mathfrak{M}$*. Handelt es sich um linksseitige Ideale, so sind entsprechend die Spalten jeder Matrix als Basis eines Moduls zu betrachten; jedes Ideal wird ein Hauptideal, für das neben A auch AV eine Basis wird, unter V eine beliebige unimodulare Matrix verstanden.

Wir legen nun im folgenden zum Zusammenhang mit der Elementarteilertheorie *zweiseitige Ideale* zugrunde, bei denen also insbesondere neben A auch PAQ zum Ideal gehört. Dann ist die allgemeinste Basis eines solchen Ideals nach dem obigen gegeben durch UAV, wo U und V unimodular sind. Die Basiselemente erschöpfen also eine *Klasse äquivalenter Matrizen*[49]), und es besteht eineindeutige Beziehung zwischen Ideal und Klasse, folglich auch zwischen Ideal und Elementarteilersystem $(a_1 \mid a_2 \mid \ldots \mid a_n)$ der Klasse, wo die a_i bekanntlich nicht-negative ganze Zahlen sind, von denen jede in der folgenden aufgeht. Die in der durch die Elementarteiler bedingten Normalform auftretende Matrix der Klasse läßt sich somit als spezielle Basis des Ideals auffassen; aus der Teilbarkeit der Ideale, bzw. Klassen folgt die der Elementarteiler, und umgekehrt.

Nun hat aber Du Pasquier a. a. O. § 11 gezeigt, daß bei jedem zweiseitigen Ideal der Rang n ist und alle Elementarteiler übereinstimmen. Um den Fall allgemeiner Elementarteiler betrachten zu können, müssen wir daher nicht von den Idealen, sondern direkt von den zweiseitigen Klassen ausgehen (die ebenfalls durch große deutsche Buchstaben bezeichnet

[49]) Den Basiselementen der einseitigen Ideale entsprechen Rechts- bzw. Linksklassen.

werden sollen). Eine Klasse $\mathfrak{A} = UAV$ ist dabei also durch eine andere $\mathfrak{B}$ teilbar, wenn $A = PBQ$ wird.

Allgemein gilt: *Das kleinste gemeinsame Vielfache (der größte gemeinsame Teiler) zweier Klassen wird erhalten durch Bildung des kleinsten gemeinsamen Vielfachen (des größten gemeinsamen Teilers) der entsprechenden Elementarteilersysteme*[50]. Denn seien $(a_1 \mid a_2 \mid \ldots a_n)$; $(b_1 \mid b_2 \ \ldots b_n)$; $(c_1 \mid c_2 \mid \ldots c_n)$, wo $c_i = [a_i, b_i]$, bzw. die Elementarteilersysteme von $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}^*$, und sei $\mathfrak{C} = [\mathfrak{A}, \mathfrak{B}]$. Dann ist $\mathfrak{C}^*$ durch $\mathfrak{A}$ und $\mathfrak{B}$, also durch $\mathfrak{C}$ teilbar, umgekehrt sind die Elementarteiler von $\mathfrak{C}$ durch die von $\mathfrak{C}^*$ teilbar, also ist $\mathfrak{C}$ durch $\mathfrak{C}^*$ teilbar und somit $\mathfrak{C} = \mathfrak{C}^*$. Entsprechend ergibt sich der Beweis für den größten gemeinsamen Teiler,

Der eindeutigen Darstellung der Elementarteiler a_i als kleinstes gemeinsames Vielfaches von Primzahlpotenzen entspricht somit eine Darstellung von $\mathfrak{A}$ als kleinstes gemeinsames Vielfaches von Klassen $\mathfrak{Q}$, deren Elementarteiler gegeben sind durch die Potenzen *einer* Primzahl, in Zeichen

$$\mathfrak{Q} \sim (p^{r_1} \mid p^{r_2} \ \ldots p^{r_\varrho} \ \ 0 \mid \ldots \mid 0); \qquad r_1 \leqq r_2 \leqq \ldots \leqq r_\varrho.$$

Ist insbesondere der Rang ϱ gleich n, so hat man hier eine Zerlegung in teilerfremde und teilerfremd-irreduzible Klassen, die trotz des nichtkommutativen Bereichs eindeutig ist.

Die Klassen $\mathfrak{Q}$ lassen sich weiter zerlegen in Klassen, die dem Elementarteilersystem ensprechen:

$$\mathfrak{B}_1 \sim (p^{r_1} \mid \ldots p^{r_1}); \quad \mathfrak{B}_2 \sim (1 \ \ p^{r_2} \ \ldots p^{r_2}); \ \ldots; \quad \mathfrak{B}_\varrho \sim (1 \mid \ldots 1 \ \ p^{r_\varrho} \ \ldots p^{r_\varrho});$$
$$\mathfrak{B}_{\varrho+1} \sim (1 \ \ \ldots 1 \mid 0 \mid \ldots 0),$$

wo in $\mathfrak{B}_\nu$ jeweils $(\nu - 1)$-mal die Zahl 1 auftritt. Ist dabei etwa $r_1 = r_2 = \ldots = r_\mu = 0$, so werden $\mathfrak{B}_1 \ldots \mathfrak{B}_\mu$ gleich der Einheitsklasse und sind folglich bei der Zerlegung wegzulassen; das gleiche gilt für $\mathfrak{B}_{\varrho+1}$, wenn $\varrho = n$ ist. Ist ferner etwa $r_\nu = r_{\nu+1} = \ldots = r_{\nu+\lambda}$, so werden $\mathfrak{B}_{\nu+1}, \ldots \mathfrak{B}_{\nu+\lambda}$ echte Teiler von $\mathfrak{B}_\nu$, sind also gleichfalls auszuscheiden. Bezeichnen $\mathfrak{B}_{i_1} \ldots \mathfrak{B}_{i_k}$ die übrigbleibenden, die jetzt eine kürzeste Darstellung ergeben, so wird $\mathfrak{Q} = [\mathfrak{B}_{i_1} \ldots \mathfrak{B}_{i_k}]$ *die eindeutige Zerlegung von* $\mathfrak{Q}$ *in irreduzible Klassen.* Sei nämlich $\mathfrak{B}_\nu \sim (1 \mid \ldots 1 \mid p^{r_\nu} \mid \ldots p^{r_\nu})$ darstellbar als kleinstes gemeinsames Vielfaches von $\mathfrak{C} \sim (1 \mid \ldots 1 \mid p^{s_1} \mid \ldots p^{s_\lambda})$ und $\mathfrak{D} \sim (1 \mid \ldots 1 \mid p^{t_1} \mid \ldots p^{t_\mu})$: dann muß im Elementarteilersystem von $\mathfrak{C}$

---

[50]) In der Arbeit: Zur Theorie der Moduln, Math. Ann. **52** (1899), S. 1 definiert E. Steinitz das kleinste gemeinsame Vielfache (den größten gemeinsamen Teiler) von Klassen durch kleinste gemeinsame Vielfache und größte gemeinsame Teiler der Elementarsysteme. Unabhängig davon findet sich das kleinste gemeinsame Vielfache von Klassen als „Kongruenzkomposition" bei H. Brandt, Komposition der binären quadratischen Formen relativ einer Grundform, J. f. M. **150** (1919), S. 1.

und $\mathfrak{D}$ an den ersten $(\nu-1)$ Stellen die Zahl 1 stehen; an ν-ter Stelle muß der Exponent s_1 oder t_1, etwa s_1, gleich r_ν werden. Da aber $r_\nu = s_1 \leqq s_2 \leqq s_\lambda \leqq r_\nu$ wird, so kommt $\mathfrak{C} = \mathfrak{B}_\nu$, also ist $\mathfrak{B}_\nu$ *irreduzibel*[51]). Dasselbe gilt für $\mathfrak{B}_{\varrho+1}$, wo p durch 0 zu ersetzen ist. Jede dieser irreduziblen Klassen gibt aber, wie die Bildung des kleinsten gemeinsamen Vielfachen zeigt, einen bestimmten Exponenten, und die Stelle, wo dieser Exponent im Elementarteilersystem von $\mathfrak{Q}$, bzw. $\mathfrak{A}$ zum erstenmal auftritt, während $\mathfrak{B}_{\varrho+1}$ den Rang angibt. Da diese Zahlen durch das Elementarteilersystem von $\mathfrak{Q}$, bzw. $\mathfrak{A}$ eindeutig festgelegt sind, und da die Beziehung zwischen Elementarteilern und Klasse eineindeutig ist, ist somit die Zerlegung von $\mathfrak{Q}$, und ebenso die einer beliebigen Klasse, in irrreduzible Klassen, *eindeutig*. Zusammenfassend läßt sich sagen: *Jede zweiseitige Klasse* $\mathfrak{A}$ *aus ganzzahligen Matrizen von beschränkter Elementenzahl läßt sich eindeutig darstellen als kleinstes gemeinsames Vielfaches von endlich vielen irreduziblen zweiseitigen Klassen. Jede irreduzible Klasse repräsentiert dabei einen festen Primteiler des Elementarteilersystems von* $\mathfrak{A}$, *einen zugehörigen Exponenten und die Stelle, wo dieser Exponent zum erstenmal auftritt. Die dem Teiler* 0 *entsprechende irreduzible Klasse gibt den Rang von* $\mathfrak{A}$ *an.*

---

[51]) Dagegen sind die $\mathfrak{B}$ noch in einseitige Klassen reduzibel; hier besteht keine eindeutige Beziehung mehr zwischen Elementarteilern und Klasse, und damit auch keine eindeutige Zerlegung in irreduzible einseitige Klassen. Das zeigt etwa das folgende mir von H. Brandt angegebene Beispiel der Zerlegung in rechtsseitige Klassen (wo die Klassen durch eine Basismatrix dargestellt sind, bzw. durch den entsprechenden Modul):

$$\mathfrak{B} = [\mathfrak{C}_1, \mathfrak{C}_2] = [\mathfrak{D}_1, \mathfrak{D}_2]; \qquad \mathfrak{B} \sim \begin{pmatrix} p & 0 \\ 0 & p \end{pmatrix}; \qquad \mathfrak{C}_1 \sim \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}; \qquad \mathfrak{C}_2 \sim \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix};$$

$$\mathfrak{D}_1 \sim \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}; \qquad \mathfrak{D}_2 \sim \begin{pmatrix} p & 0 \\ (p-1) & 1 \end{pmatrix}.$$

In der Tat besitzen die Moduln $(\xi, p\eta)$; $(p\xi, \eta)$; $(p\xi, (p-1)\xi + \eta)$ jeweils als echten Teiler nur den Modul (ξ, η), sind also irreduzibel und sind ferner voneinander verschieden.

Erlangen, Oktober 1920.

(Eingegangen am 16. 10. 1920.)