Axiomatische Begründung der allgemeinen Idealtheorie.

Von

Wolfgang Krull.

In der vorliegenden Arbeit sollen auf neuem, axiomatischem Wege die folgenden Hauptsätze der allgemeinen Idealtheorie abgeleitet werden[1]): „Zu jedem Ideal gibt es endlich viel „zugehörige Primideale“ und „isolierte Komponentenideale“. Jedes isolierte Komponentenideal steht in eindeutig umkehrbarer Beziehung zu einer gewissen Schar zugehöriger Primideale.“ Außerdem werden die bekannten Ergebnisse in verschiedener Hinsicht erweitert und vertieft. Im Gegensatz zu den bisherigen Darstellungen werden die Ideale nicht mit Hilfe des Ringbegriffs eingeführt, sondern allein durch die axiomatisch festgelegten Teilbarkeits- und Multiplikationseigenschaften charakterisiert. Auch im übrigen verläuft der Beweisgang gerade umgekehrt wie in den unten zitierten Arbeiten N. und K. Dort wurde zunächst die Zerlegbarkeit jedes Ideals in Primärkomponenten nachgewiesen, das gewonnene Ergebnis ermöglichte dann die Definition der zugehörigen Primideale und isolierten Komponentenideale, sowie die Ermittlung ihrer hauptsächlichen Eigenschaften. In der vorliegenden Arbeit hingegen werden zugehörige Primideale und isolierte Komponentenideale durch die am Schlusse von K. angegebenen charakteristischen Eigenschaften eingeführt, und es werden dann mit Hilfe dieser Definitionen die oben angegebenen Hauptsätze abgeleitet, unter

1) Vgl. zum Thema die grundlegende Arbeit von E. Noether: Idealtheorie in Ringbereichen, Math. Annal. 83 (1921), S. 23—66 (in Zukunft kurz mit N. zitiert), sowie Krull: Ein neuer Beweis für die Hauptsätze der allgemeinen Idealtheorie, Math. Annal. 90 (1923), S. 55—64 (in Zukunft kurz mit K. zitiert).

völliger Vermeidung der — bekanntlich nicht eindeutig bestimmten — Zerlegung eines Ideals in Primärkomponenten.

Der hier skizzierte Weg ergibt sich naturgemäß aus dem axiomatischen Ausgangspunkt; er erfordert nirgends ein Rechnen mit Elementen und hat den Vorteil, daß die eindeutig bestimmten Begriffe des zugehörigen Primideals und des isolierten Komponentenideals von vornherein in den Vordergrund treten.

Nur in lockerem Zusammenhang mit den übrigen Untersuchungen steht § 6. In ihm werden kurz die bekannten charakteristischen Eigenschaften der teilerfremden Ideale abgeleitet, insbesondere wird ein neuer Beweis für die eindeutige Zerlegbarkeit jedes Ideals in teilerfremd-irreduzible Faktoren gegeben.

Charakteristisch für die Darstellung ist die starke Verwendung des für Ideale gültigen Rechenformalismus, durch den viele Beweise sehr kurz und einfach werden.

§ 1. Axiome, Definitionen und Rechenregeln.

Den Untersuchungen liegt ein Bereich zugrunde, dessen Elemente Ideale genannt und mit kleinen deutschen Buchstaben bezeichnet werden. Es gelten folgende Axiome:

I. Teilbarkeitsaxiome.

(Entsprechen denjenigen Axiomen der Mengenlehre, bei denen es sich um Enthaltensein, Durchschnitts- und Vereinigungsmenge handelt.)

a) Es sind zwei Beziehungen $<$ und $>$ mit folgenden Eigenschaften erklärt:

α) Aus $\mathfrak{a} < \mathfrak{b}$ folgt $\mathfrak{b} > \mathfrak{a}$.

β) $\mathfrak{a} < \mathfrak{a}$, $\mathfrak{a} > \mathfrak{a}$; ist umgekehrt $\mathfrak{a} < \mathfrak{b}$, $\mathfrak{b} < \mathfrak{a}$, so ist $\mathfrak{b} = \mathfrak{a}$ [2]).

γ) Ist $\mathfrak{a} < \mathfrak{b}$, $\mathfrak{b} < \mathfrak{c}$, so ist $\mathfrak{a} < \mathfrak{c}$.

Ist $\mathfrak{a} < \mathfrak{b}$, so nennen wir $\mathfrak{b}$ „durch $\mathfrak{a}$ teilbar“ oder „Vielfaches von $\mathfrak{a}$“, $\mathfrak{a}$ wird als „Teiler von $\mathfrak{b}$“ bezeichnet; sind $\mathfrak{a}$ und $\mathfrak{b}$ verschieden, so reden wir von „echtem Vielfachen“ bezw. „echtem Teiler“. Ist $\mathfrak{b}$ ein echtes oder unechtes Vielfaches von $\mathfrak{a}$, so schreiben wir in Zukunft stets $\mathfrak{a} \leqq \mathfrak{b}$; $\mathfrak{b} \geqq \mathfrak{a}$.

2) Mit Hilfe von β) kann man geradezu die Gleichheit zweier Ideale unseres Bereiches definieren.

Die Schreibweise $a < b$, $b > a$ verwenden wir nur dann, wenn a und b sicher verschieden sind. Besonders betont möge werden, daß für beliebige Ideale a und b nicht notwendig eine der beiden Beziehungen $a < b$, $a > b$ gelten muß.

b) Zu zwei beliebigen Idealen a_1 und a_2 gibt es einen „größten gemeinschaftlichen Teiler“ (a_1, a_2) und ein „kleinstes gemeinschaftliches Vielfaches $[a_1, a_2]$ mit folgenden Eigenschaften:

(a_1, a_2) ($[a_1, a_2]$) ist gemeinschaftlicher Teiler (gemeinschaftliches Vielfaches) von a_1 und a_2: jeder gemeinschaftliche Teiler (jedes gemeinschaftliche Vielfache) von a_1 und a_2 ist Teiler von (a_1, a_2) (Vielfaches von $[a_1, a_2]$). In Formeln haben wir also:

$a_1 \geqq (a_1, a_2)$; $a_2 \geqq (a_1, a_2)$; aus $a_1 > b$: $a_2 \geqq b$ folgt $(a_1, a_2) \geqq b$.

$a_1 \leqq [a_1, a_2]$; $a_2 \leqq [a_1, a_2]$; aus $a_1 < b$: $a_2 \leqq b$ folgt $[a_1, a_2] \leqq b$.

Nachdem die Existenz von (a_1, a_2) und $[a_1, a_2]$ axiomatisch feststeht, kann das Vorhandensein eines ganz analog definierten größten gemeinschaftlichen Teilers $(a_1, a_2, \ldots a_n)$ bezw. eines kleinsten gemeinschaftlichen Vielfachen $[a_1, a_2, \ldots a_n]$ von endlich viel Idealen bewiesen werden.

$(a_1, a_2 \ldots a_n)$ erhält man z. B., wenn man der Reihe nach die Ideale (a_1, a_2), $((a_1, a_2), a_3)$, $(((a_1, a_2), a_3), a_4)$, ... bildet.

Es sei noch folgende Tatsache erwähnt, die sich leicht aus der Definition von (a_1, a_2) bezw. $[a_1, a_2]$ ergibt: Es ist $(a_1, a_2) = a_1$ bezw. $[a_1, a_2] = a_1$ dann und nur dann, wenn $a_2 \geqq a_1$ bezw. $a_2 \leqq a_1$.

c) Auch zu einer unendlichen Menge von Idealen gibt es stets einen größten gemeinschaftlichen Teiler. Insbesondere muß also ein Ideal o existieren, das Teiler aller Ideale unseres Bereiches ist. o wird als „Einheitsideal“ bezeichnet.

II. Axiom der Multiplikation.

Aus je zwei Idealen a und b kann mit Hilfe einer assoziativen und kommutativen, als „Multiplikation“ bezeichneten Operation ein neues Ideal $a \cdot b$ abgeleitet werden. Dabei ist:

$$a \cdot b \geqq [a, b] \tag{1}$$

$$a \cdot (b_1, b_2, \ldots) = (a \cdot b_1, a \cdot b_2, \ldots) \tag{2}$$

Formel (2), das „distributive Gesetz“, soll auch dann gelten, wenn es sich bei $(\mathfrak{b}_1, \mathfrak{b}_2 \ldots)$ um den größten gemeinschaftlichen Teiler einer beliebigen unendlichen Idealmenge handelt.

Ist $\mathfrak{b}_1 \geqq \mathfrak{b}_2$, so haben wir $(\mathfrak{b}_1, \mathfrak{b}_2) = \mathfrak{b}_2$; $\mathfrak{a} \cdot (\mathfrak{b}_1, \mathfrak{b}_2) = (\mathfrak{a}\cdot\mathfrak{b}_1, \mathfrak{a}\cdot\mathfrak{b}_2) = \mathfrak{a}\cdot\mathfrak{b}_2$, d. h. $\mathfrak{a}\cdot\mathfrak{b}_1 \geqq \mathfrak{a}\cdot\mathfrak{b}_2$.

Nach axiomatischer Festlegung der Idealmultiplikation führen wir nunmehr durch Definition den Idealquotienten ein:

Definition: Der Quotient $\mathfrak{a}:\mathfrak{b}$ ist der größte gemeinschaftliche Teiler aller der Ideale $\mathfrak{c}$, für die $\mathfrak{b}\cdot\mathfrak{c} \geqq \mathfrak{a}$ ist.

Aus unseren Axiomen, insbesondere aus Formel (1) und (2) ergeben sich für den Idealquotienten folgende Eigenschaften:

$$\mathfrak{b}\cdot(\mathfrak{a}:\mathfrak{b}) \geqq \mathfrak{a};\quad \mathfrak{a}:\mathfrak{b} \leqq \mathfrak{a};\quad \mathfrak{a}:\mathfrak{b}_1 \leqq \mathfrak{a}:\mathfrak{b}_2, \text{ wenn } \mathfrak{b}_1 \geqq \mathfrak{b}_2;$$

$$\mathfrak{a}:\mathfrak{b} = \mathfrak{o}, \text{ wenn } \mathfrak{b} \geqq \mathfrak{a}. \tag{3}$$

$$\mathfrak{a}:(\mathfrak{b}_1\cdot\mathfrak{b}_2) = (\mathfrak{a}:\mathfrak{b}_1):\mathfrak{b}_2 = (\mathfrak{a}:\mathfrak{b}_2):\mathfrak{b}_1, \tag{4}$$

$$[\mathfrak{a}_1, \mathfrak{a}_2, \ldots \mathfrak{a}_n]:\mathfrak{b} = [\mathfrak{a}_1:\mathfrak{b}, \mathfrak{a}_2:\mathfrak{b}, \ldots \mathfrak{a}_n:\mathfrak{b}]. \tag{5}$$

$$\mathfrak{a}:(\mathfrak{b}_1, \mathfrak{b}_2, \ldots \mathfrak{b}_n) = [\mathfrak{a}:\mathfrak{b}_1, \mathfrak{a}:\mathfrak{b}_2, \ldots \mathfrak{a}:\mathfrak{b}_n]. \tag{6}$$

Wir unterdrücken die einfachen Beweise der angeschriebenen Formeln, weil sie sich bereits an anderer Stelle[3]) in der Literatur finden.

Definition: Ist $\mathfrak{a}:\mathfrak{b} = \mathfrak{a}$, so heißt $\mathfrak{b}$ „zu $\mathfrak{a}$ prim“. Ist $\mathfrak{a}:\mathfrak{b} = \mathfrak{a}$, $\mathfrak{b}:\mathfrak{a} = \mathfrak{b}$, so heißen $\mathfrak{a}$ und $\mathfrak{b}$ „gegenseitig prim“.

Aus Formel (4) folgt unmittelbar, daß $\mathfrak{b}_1\cdot\mathfrak{b}_2$ (und folglich a fortiorio $[\mathfrak{b}_1, \mathfrak{b}_2]$) dann und nur dann zu $\mathfrak{a}$ prim ist, wenn das gleiche von $\mathfrak{b}_1$ und $\mathfrak{b}_2$ gilt.

Definition: Ein Ideal $\mathfrak{p}$ heißt Primideal, wenn für beliebiges $\mathfrak{a}$ stets entweder $\mathfrak{a} \geqq \mathfrak{p}$ oder $\mathfrak{p}:\mathfrak{a} = \mathfrak{p}$ ist, d. h. wenn aus $\mathfrak{a}_1\cdot\mathfrak{a}_2 \geqq \mathfrak{p}$ stets die Gültigkeit einer der Gleichungen $\mathfrak{a}_1 \geqq \mathfrak{p}$ bezw. $\mathfrak{a}_2 \geqq \mathfrak{p}$ folgt.

III. Endlichkeitsaxiom.

Eine „echte Teilerkette“ $\mathfrak{a}_1 > \mathfrak{a}_2 > \mathfrak{a}_3 > \ldots$ bricht stets nach endlich viel Schritten ab[4]).

3) Vgl. insbesondere: Dedekind: Supplemente zu Dirichlets Vorlesungen über Zahlentheorie, IV. Aufl., p. 504, wo die entsprechenden Formeln für Moduln abgeleitet sind. Vgl. ferner Macaulay, Cambridge Tracts Nr. 19 (1916). Cap. III art. 24 u. 28, sowie K. § 2.

4) Nimmt man das Endlichkeitsaxiom zu den Axiomen I a u. I b hinzu, so wird I c ein beweisbarer Lehrsatz. Die Anordnung des Textes, bei der

Axiom III bildet die Grundlage unserer Existenzbeweise, und zwar verwenden wir vor allem folgenden Schluß:

Kann aus der Tatsache, daß eine Eigenschaft A einem beliebigen Ideal a_1 zukommt, gefolgert werden, daß A auch einem echten Teiler a_2 von a_1 zukommen muß, so kann A überhaupt keinem Ideale zukommen, weil es andernfalls eine ins Unendliche laufende echte Teilerkette $a_1 > a_2 > a_3 > \ldots$ gäbe, bei der A jedem der Ideale a_i zukäme.

§ 2. Isolierte Komponentenideale und zugehörige Primideale.

Definition: Ein Ideal i heißt „isoliertes Komponentenideal“ (in Zukunft kurz „i. K.-I.“) von a, wenn ein Ideal b existiert, das der Gleichung $a : b^r = a : b^{r+1} = \ldots = i$ genügt. Ferner soll a selbst stets als i. K.-I. von a angesehen werden[5]).

Da in der Kette $a : b$, $a : b^2$, ... stets $a : b^i \geqq a : b^{i+1}$ ist, so folgt aus dem Endlichkeitsaxiom, daß jedes Ideal b ein i. K.-I. von a „erzeugt“. Das durch b erzeugte i. K.-I. von a werde mit $i_b^{(a)}$ oder, falls keine Verwechslung zu befürchten ist, mit i_b bezeichnet. Es gilt nun:

$$i_{(b_1,\ b_2)} = [i_{b_1},\ i_{b_2}] \tag{7}$$

$$i_{(a_1 \cdot b_2)} = i_{(b_1,\ b_2)} = i_{b_1} = i_{b_2},\ i_{(b_1 \cdot b)} = i_{(b_2 \cdot b)},\ \text{wenn } i_{b_1} = i_{b_2} \tag{8}$$

Es sei r so groß gewählt, daß $i_{b_k} = a : b_k^r$; $i_{(b_k \cdot b)} = a : (b_k \cdot b)^r$ $(k = 1,2)$ wird. Dann ist für $s \geqq 2r$ stets $a : (b_1,\ b_2)^s = a : (\ldots, b_1^i \cdot b_2^k, \ldots) = [\ldots,\ a : (b_1^i \cdot b_2^k),\ \ldots] = [i_{b_1},\ i_{b_2}] = i_{(b_1,\ b_2)}$[6]) $(i + k = s)$. Ist ferner $i_{b_1} = i_{b_2}$, so haben wir für $s \geqq r$ die Gleichungen: $a : (b_1 \cdot b_2)^s = (a : b_1^s) : b_2^s = i_{b_1} : b_2^s = i_{b_1} = i_{b_2}$; $a : (b_1 \cdot b)^s = (a : b_1^s) : b^s = (a : b_2^s) : b^s = a : (b_2 \cdot b)^s$.

Definition: Ein Primideal p heißt „zu a gehörig“, wenn $i_p < a$: $a : i_p > p$ ist.

---

nicht alle Axiome unabhängig sind, soll die Sonderstellung des Endlichkeitsaxioms hervorheben.

5) Genügt das Einheitsideal o nicht der Gleichung $a \cdot o = a$ für bel. a, so kann es sehr wohl vorkommen, daß für bel. b stets $a : b < a$ wird. Die letzte Festsetzung unserer Definition ist mithin nicht überflüssig.

6) Man beachte die aus Formel (4) folgenden Beziehungen: $a : b_1^s = i_{b_1}$; $a : b_2^s = i_{b_2}$; $a : (b_1^i \cdot b_2^k) \leq i_{b_1}$ $(i \geq r)$; $a : (b_1^i \cdot b_2^k) \leq i_{b_2}$ $(k \geq r)$!

Zusatz: Das zugehörige Primideal kann auch folgendermaßen definiert werden:

Das Primideal $\mathfrak{p}$ gehört zu $\mathfrak{a}$, wenn aus $i_\mathfrak{b} = i_\mathfrak{p} < \mathfrak{a}$ stets $\mathfrak{b} \geqq \mathfrak{p}$ folgt.

Das Primideal $\mathfrak{p}$ gehört zu $\mathfrak{a}$, wenn aus $\mathfrak{b} < \mathfrak{p}$ stets $\mathfrak{a} \geqq i_\mathfrak{b} > i_\mathfrak{p}$ folgt.

Die Äquivalenz der zweiten und dritten Definition ergibt sich aus Formel (7). Ist ferner $i_\mathfrak{b} = i_\mathfrak{p}$, so haben wir (für genügend großes r) $\mathfrak{b}^r \cdot i_\mathfrak{p} \geqq \mathfrak{a}$, aus $i_\mathfrak{b} = i_\mathfrak{p}$, $\mathfrak{a} : i_\mathfrak{p} \geqq \mathfrak{p}$ folgt also $\mathfrak{b}^r \geqq \mathfrak{p}$ und mithin wegen der Primidealeigenschaft von $\mathfrak{p}$ auch $\mathfrak{b} \geqq \mathfrak{p}$. Sollte schließlich $\mathfrak{a} : i_\mathfrak{p}$ nicht durch $\mathfrak{p}$ teilbar sein, so haben wir für $\mathfrak{b} = (\mathfrak{a} : i_\mathfrak{p}, \mathfrak{p})$ die Beziehungen $\mathfrak{b} < \mathfrak{p}$, $i_\mathfrak{b} = i_\mathfrak{p}$.

Aus der dritten Definition ergibt sich angesichts der Gleichung $i_\mathfrak{p} = i_{(\mathfrak{a}, \mathfrak{p})}$:

Jedes zu $\mathfrak{a}$ gehörige Primideal ist Teiler von $\mathfrak{a}$.

Es soll jetzt bewiesen werden, daß zu jedem Ideal $\mathfrak{a} \neq \mathfrak{o}$ mindestens eines, aber sicher nur endlich viele Primideale gehören.

Hilfssatz 1. Zu jedem Ideal $\mathfrak{a}$ gibt es endlich viele Primideale $\mathfrak{p}_i \leqq \mathfrak{a}$, derart daß $\Pi \mathfrak{p}_i \geqq \mathfrak{a}$ wird.

Ist $\mathfrak{a}$ Primideal, so ist die Behauptung klar. Im andern Fall gibt es zwei durch $\mathfrak{a}$ unteilbare Ideale $\mathfrak{a}_1'$ und $\mathfrak{a}_2'$, für die $\mathfrak{a}_1' \cdot \mathfrak{a}_2' \geqq \mathfrak{a}$ wird. Dann ist aber auch $(\mathfrak{a}_1', \mathfrak{a}) \cdot (\mathfrak{a}_2', \mathfrak{a}) \geqq \mathfrak{a}$, und hier sind $\mathfrak{a}_1 = (\mathfrak{a}_1', \mathfrak{a})$ und $\mathfrak{a}_2 = (\mathfrak{a}_2', \mathfrak{a})$ echte Teiler von $\mathfrak{a}$. Gilt nun Hilfssatz 1 für $\mathfrak{a}_1$ und $\mathfrak{a}_2$, so gilt er auch für $\mathfrak{a}$, d. h. ist er für $\mathfrak{a}$ falsch, so ist er auch für einen echten Teiler von $\mathfrak{a}$ (nämlich für $\mathfrak{a}_1$ oder $\mathfrak{a}_2$) falsch. Aus dieser Überlegung folgt aber nach dem Korollar zum Endlichkeitsaxiom die Gültigkeit des Hilfssatzes für bel. $\mathfrak{a}$.

Satz 1. Es ist $\mathfrak{a} : \mathfrak{b} < \mathfrak{a}$ dann und nur dann, wenn $\mathfrak{b}$ durch ein zu $\mathfrak{a}$ gehöriges Primideal teilbar ist.

Ist zunächt $\mathfrak{p}$ ein zu $\mathfrak{a}$ gehöriges Primideal und $\mathfrak{b} > \mathfrak{a}$, so ist $i_\mathfrak{b} < i_\mathfrak{p}$ und mithin sicher von $\mathfrak{a}$ verschieden. Die Umkehrung beweisen wir negativ, indem wir zeigen, daß aus der Annahme eines zu $\mathfrak{a}$ nicht primen, aber durch kein zu $\mathfrak{a}$ gehöriges Primideal teilbaren Ideales $\mathfrak{b}$ die Existenz eines echten Teilers $\mathfrak{b}_1$ von $\mathfrak{b}$ folgt, der offenbar durch kein zu $\mathfrak{a}$ gehöriges Primideal teilbar ist, und für den gleichfalls $\mathfrak{a} : \mathfrak{b}_1 < \mathfrak{a}$ wird.

in der Tat, ist $\mathfrak{b}$ Primideal, so ist die Existenz von $\mathfrak{b}_1$ gesichert, weil sonst $\mathfrak{b}$ nach Definition selbst zu $\mathfrak{a}$ gehörte. Im andern Falle können wir nach Hilfssatz 1 r Primideale $\mathfrak{p}_1$, $\mathfrak{p}_2$, . . . $\mathfrak{p}_r$ bestimmen, die hier echte Teiler von $\mathfrak{a}$ sind, und für die $\prod_{i=1}^{r} \mathfrak{p}_i \geqq \mathfrak{b}$ wird. Dann aber ist $(\mathfrak{a} : \prod \mathfrak{p}_i) \leqq \mathfrak{a} : \mathfrak{b} < \mathfrak{a}$, und mithin nach Formel (4) auch für eines der $\mathfrak{p}_i$ sicher $\mathfrak{a} : \mathfrak{p}_i < \mathfrak{a}$.

Da für beliebiges $\mathfrak{a} \neq \mathfrak{o}$ stets $\mathfrak{a} : \mathfrak{a} = \mathfrak{o} < \mathfrak{a}$ ist, so folgt aus Satz 1 unmittelbar:

Satz 2. Jedes von $\mathfrak{o}$ verschiedene Ideal besitzt mindestens ein zugehöriges Primideal.

Satz 3. Zu jedem Ideal $\mathfrak{a}$ gehören nur endlich viele Primideale.

Bei dem in 6 Schritten zu führenden Beweis bedeutet $\mathfrak{p}$ stets ein zu $\mathfrak{a}$ gehöriges Primideal.

α) Jede Kette $\mathfrak{p}_1 > \mathfrak{p}_2 > \mathfrak{p}_3 > \ldots$ besitzt nach dem Endlichkeitsaxiom nur endlich viele Glieder.

β) Jede Kette $\mathfrak{p}_1 < \mathfrak{p}_2 < \mathfrak{p}_3 < \ldots$ besitzt nur endlich viele Glieder, weil aus ihr die Kette $i_{\mathfrak{p}_1} > i_{\mathfrak{p}_2} > i_{\mathfrak{p}_3} > \ldots$ abgeleitet werden kann. (Definition des zugehörigen Primideals!)

γ) Jede Kette $\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3, \ldots$, bei der kein $\mathfrak{p}_i$ durch ein $\mathfrak{p}_k$ $(i \neq k)$ teilbar ist, besitzt nur endlich viele Glieder, weil aus ihr die Kette $i_{\mathfrak{p}_1} > i_{(\mathfrak{p}_1 \cdot \mathfrak{p}_2)} > i_{(\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3)} > \ldots$ abgeleitet werden kann.

In der Tat, zunächst ist $i_{(\mathfrak{p}_1 \cdot \mathfrak{p}_2 \ldots \mathfrak{p}_{r-1})} \geqq i_{(\mathfrak{p}_1 \cdot \mathfrak{p}_2 \ldots \mathfrak{p}_r)}$; gälte das Gleichheitszeichen, so hätten wir wegen $i_{\mathfrak{p}_r} \geqq i_{(\mathfrak{p} \cdot \mathfrak{p}_2 \ldots \mathfrak{p}_r)}$ und Formel (7) sicher $i_{(\mathfrak{p}_1 \ldots \mathfrak{p}_{r-1}, \mathfrak{p}_r)} = i_{\mathfrak{p}_r}$. Diese letztere Gleichung ist aber unmöglich, weil bei unseren Annahmen über die zu $\mathfrak{a}$ gehörigen Primideale $\mathfrak{p}_i$ sicher $(\mathfrak{p}_1 \cdot \mathfrak{p}_2 \ldots \mathfrak{p}_{r-1}, \mathfrak{p}_r) < \mathfrak{p}_r$ ist.

δ) Zu jedem $\mathfrak{p}$ gibt es eine natürliche Zahl s, die als die „Stufe von $\mathfrak{p}$" bezeichnet wird, und die dadurch charakterisiert ist, daß keine Kette $\mathfrak{p} > \mathfrak{p}_1 > \mathfrak{p}_2 > \ldots$ mehr als $s+1$ Glieder besitzt, während mindestens eine $s+1$ gliedrige derartige Kette wirklich auftritt.

Gibt es kein $\mathfrak{p}_1$, für das $\mathfrak{p} > \mathfrak{p}_1$ ist, so besitzt $\mathfrak{p}$ nach Definition die Stufe 1. Im andern Falle existieren end-

lich viele Ideale $\mathfrak{p}_1, \mathfrak{p}_2 \ldots \mathfrak{p}_r$, für die $\mathfrak{p} > \mathfrak{p}_i$ $(i = 1, 2 \ldots r)$ ist, und die außerdem die Eigenschaft besitzen, daß es kein der Beziehung $\mathfrak{p} > \mathfrak{p}' > \mathfrak{p}_i$ genügendes $\mathfrak{p}'$ gibt. (Daß die Ideale $\mathfrak{p}_i$ nur in endlicher Anzahl vorhanden sein können, folgt aus γ); daß mindestens ein $\mathfrak{p}_i$ existiert, erkennt man aus β), indem man von einem beliebigen der Ungleichung $\mathfrak{p} > \mathfrak{p}'$ genügenden Ideale $\mathfrak{p}'$ ausgeht, und eine Kette $\mathfrak{p}', \mathfrak{p}'', \ldots$ bildet, bei der allgemein $\mathfrak{p}^{(k)} > \mathfrak{p}^{(k-1)}$; $\mathfrak{p} > \mathfrak{p}^{(k)}$ ist.) Besitzt nun jedes der Ideale $\mathfrak{p}_i$ eine endliche Stufe s_i, so besitzt $\mathfrak{p}$ offenbar die Stufe $\max(s_i) + 1$ $(i = 1, 2 \ldots r)$. Die Annahme, $\mathfrak{p}$ besäße keine Stufe, führt also zu der Folgerung, daß das gleiche von einem echten Teiler $\mathfrak{p}_i$ gelten muß, und mithin schließlich zu einem Widerspruch gegen das Endlichkeitsaxiom. — Wir erwähnen noch einige wichtige Folgerungen aus der Stufendefinition.

Jedes Ideal s^{ter} Stufe ist durch mindestens ein Ideal $s-1^{ter}$ Stufe teilbar. Ist s_1 die Stufe von $\mathfrak{p}_1$, s_2 diejenige von $\mathfrak{p}_2$, so folgt aus $\mathfrak{p}_1 > \mathfrak{p}_2$ stets $s_1 > s_2$. Zwei Ideale gleicher Stufe sind gegenseitig prim, es gibt also nur endlich viel Ideale einer festen Stufe.

ε) Für die Stufe s eines zu $\mathfrak{a}$ gehörigen Primideals existiert eine obere Schranke s_o.

Wir wollen unter einem „höchsten Primideal von $\mathfrak{a}$" ein solches $\mathfrak{p}$ verstehen, das unter den Primidealen von $\mathfrak{a}$ kein echtes Vielfaches besitzt. Aus γ) folgt, daß es nur endlich viel Primideale höchster Stufe geben kann, und aus β) läßt sich schließen, daß jedes $\mathfrak{p}$ in mindestens einem Primideal höchster Stufe aufgeht. Sind daher $\mathfrak{p}_1, \mathfrak{p}_2, \ldots \mathfrak{p}_r$ die höchsten Primideale von $\mathfrak{a}$, und bezeichnet s_i die Stufe von $\mathfrak{p}_i$, so gilt für die Stufe s eines bel. $\mathfrak{p}$ die Ungleichung $s \leqq \max \cdot (s_i) = s_o$.

ζ) Bedeutet r_s die Anzahl der Primideale s^{ter} Stufe, so beträgt die Gesamtzahl der zu $\mathfrak{a}$ gehörigen Primideale $r = \sum_{s=1}^{s_o} r_s$.

Hiermit ist Satz 3 bewiesen, und gleichzeitig der Begriff der „Stufe eines Primideals" sowie eines „höchsten Primideals von $\mathfrak{a}$" gewonnen. Die Primideale erster Stufe sollen auch „niederste Primideale von $\mathfrak{a}$" heißen.

§ 3. Bestimmung sämtlicher i. K.-I. von $\mathfrak{a}$.

Satz 4. Zu $\mathfrak{a} : \mathfrak{b} = \mathfrak{b}$ gehören stets nur solche Primideale, die auch zu $\mathfrak{a}$ gehören, und insbesondere alle zu $\mathfrak{a}$ gehörigen und nicht in $\mathfrak{b}$ aufgehenden Primideale.

α) Es sei $\mathfrak{p}$ ein zu $\mathfrak{b}$ gehöriges Primideal, und r so groß gewählt, daß $i_{\mathfrak{p}}^{(\mathfrak{a})} = \mathfrak{a} : \mathfrak{p}^r$; $i_{\mathfrak{p}}^{(\mathfrak{b})} = \mathfrak{b} : \mathfrak{p}^r = \mathfrak{a} : (\mathfrak{b} \cdot \mathfrak{p}^r)$ wird. Dann ist $i_{\mathfrak{p}}^{(\mathfrak{a})} < \mathfrak{a}$, weil andernfalls $i_{\mathfrak{p}}^{(\mathfrak{b})} = \mathfrak{a} : (\mathfrak{b} \cdot \mathfrak{p}^r) = (\mathfrak{a} : \mathfrak{p}^r) : \mathfrak{b} = \mathfrak{b}$ wäre. Ferner haben wir $\mathfrak{b} : i_{\mathfrak{p}}^{(\mathfrak{b})} = (\mathfrak{a} : \mathfrak{b}) : (\mathfrak{a} : (\mathfrak{b} \cdot \mathfrak{p}^r)) = \mathfrak{a} : [\mathfrak{b} \cdot ((\mathfrak{a} : \mathfrak{p}^r) : \mathfrak{b})] < \mathfrak{a} : (\mathfrak{a} : \mathfrak{p}^r) = \mathfrak{a} : i_{\mathfrak{p}}^{(\mathfrak{a})}$, es folgt also aus $\mathfrak{b} : i_{\mathfrak{p}}^{(\mathfrak{b})} > \mathfrak{p}$ sicher $\mathfrak{a} : i_{\mathfrak{p}}^{(\mathfrak{a})} \geqq \mathfrak{p}$.

β) Es sei umgekehrt $\mathfrak{p}$ ein zu $\mathfrak{a}$ gehöriges Primideal und $(\mathfrak{b}, \mathfrak{p}) < \mathfrak{p}$: $i_{\mathfrak{p}}^{(\mathfrak{a})} = \mathfrak{a} : \mathfrak{p}^r$, $i_{\mathfrak{p}}^{(\mathfrak{b})} = \mathfrak{b} : \mathfrak{p}^r = \mathfrak{a} : (\mathfrak{b} \cdot \mathfrak{p}^r)$. Dann ist $i_{\mathfrak{p}}^{(\mathfrak{b})} < \mathfrak{b}$, weil andernfalls $i_{\mathfrak{p}}^{(\mathfrak{a})} \geqq i_{\mathfrak{p}}^{(\mathfrak{b})} = \mathfrak{a} : \mathfrak{b}$, mithin $i_{\mathfrak{p}}^{(\mathfrak{a})} = \mathfrak{a} : (\mathfrak{p}^r, \mathfrak{b})$ wäre, also $\mathfrak{p}$ nicht zu $\mathfrak{a}$ gehörte. Ferner haben wir: $\mathfrak{b} \cdot (\mathfrak{b} : i_{\mathfrak{p}}^{(\mathfrak{b})}) = \mathfrak{b} \cdot [(\mathfrak{a} : \mathfrak{b}) : (\mathfrak{a} : (\mathfrak{b} \cdot \mathfrak{p}^r))] = \mathfrak{b} \cdot [(\mathfrak{a} : (\mathfrak{a} : (\mathfrak{b} \cdot \mathfrak{p}^r))) : \mathfrak{b}] \geqq \mathfrak{a} : (\mathfrak{a} : (\mathfrak{b} \cdot \mathfrak{p}^r)) \geqq \mathfrak{a} : (\mathfrak{a} : \mathfrak{p}^r) = \mathfrak{a} : i_{\mathfrak{p}}^{(\mathfrak{a})}$. Aus $\mathfrak{a} : i_{\mathfrak{p}}^{(\mathfrak{a})} \geqq \mathfrak{p}$ folgt daher $\mathfrak{b} \cdot (\mathfrak{b} : i_{\mathfrak{p}}^{(\mathfrak{b})}) \geqq \mathfrak{p}$ und mithin wegen $\mathfrak{p} : \mathfrak{b} = \mathfrak{p}$ auch $\mathfrak{b} : i_{\mathfrak{p}}^{(\mathfrak{b})} \geqq \mathfrak{p}$.

Da $\mathfrak{a} : \mathfrak{b} < \mathfrak{a}$ wird, falls $\mathfrak{b}$ durch ein zu $\mathfrak{a}$ gehöriges Primideal teilbar ist, so folgt aus Satz 4:

Satz 5. Zu $i_{\mathfrak{b}}^{(\mathfrak{a})}$ gehören alle und nur die Primideale, die zu $\mathfrak{a}$ gehören, und nicht Teiler von $\mathfrak{b}$ sind.

Aus Satz 5 ergibt sich:

Hilfssatz 2. Bedeutet r das Produkt der höchsten Primideale von $\mathfrak{a}$, so wird für genügend großes r: $r^r \geqq \mathfrak{a}$.

In der Tat, wählen wir r hinreichend groß, so wird $\mathfrak{a} : r^{r-1} = i_r = o$, und mithin $o \cdot r^{r-1} \geqq \mathfrak{a}$, also auch $r^r \geqq \mathfrak{a}$. Aus dem Hilfssatz folgt, daß zwei Ideale $\mathfrak{b}_1$ und $\mathfrak{b}_2$ mit denselben höchsten Primidealen stets das gleiche i. K.-I. von $\mathfrak{a}$ erzeugen: denn bezeichnen wir mit r das Produkt jener höchsten Primideale, so wird für genügend großes r: $r^r \geqq [\mathfrak{b}_1, \mathfrak{b}_2]$; $(\mathfrak{b}_1, \mathfrak{b}_2)^r \geqq r$, und mithin $i_{\mathfrak{b}_1} = i_{\mathfrak{b}_2} = i_r$.

Um mit Hilfe der gewonnenen Resultate einen Überblick über die i. K.-I. von $\mathfrak{a}$ zu gewinnen, führen wir folgende Bezeichnungsweise ein:

Eine Schar S zu $\mathfrak{a}$ gehöriger Primideale heißt „isolierte Schar“, wenn mit $\mathfrak{p}$ gleichzeitig jedes der Beziehung $\mathfrak{p}' > \mathfrak{p}$

genügende Primideal der Schar angehört[7]). Ein Primideal $\mathfrak{p}$ von $\mathfrak{a}$ heißt „höchstes Primideal außerhalb von S", wenn $\mathfrak{p}$ der Schar S nicht angehört, und wenn es außerhalb von S kein echtes Vielfaches von $\mathfrak{p}$ unter den zu $\mathfrak{a}$ gehörigen Primidealen gibt.

Der Durchschnitt und die Vereinigungsschar[8]) zweier isolierter Scharen S_1 und S_2 ist stets wieder eine isolierte Schar. Ferner bildet die Gesamtheit aller zu $\mathfrak{a}$ gehörigen Primideale, die in einem bestimmten Ideal $\mathfrak{b}$ nicht aufgehen, eine isolierte Schar. Auf Grund dieser letzteren Tatsache und mit Hilfe von Satz 5 beweisen wir:

Satz 6. Zu jeder isolierten Primidealschar von $\mathfrak{a}$ gibt es ein und nur ein i. K.-I., zu dem gerade die Primideale jener Schar gehören, und umgekehrt.

Zunächst ist nach Satz 5 klar, daß die Primideale eines i. K.-I. von $\mathfrak{a}$ eine isolierte Schar bilden. Ferner gehört auch zu jeder isolierten Schar mindestens ein i. K.-I., nämlich zu der Schar S^x aller Primideale von $\mathfrak{a}$ einzig das Ideal $\mathfrak{a}$ selbst, und zu jeder von S^x verschiedenen Schar S jedenfalls dasjenige i. K.-I., das durch das Produkt der höchsten Primideale von $\mathfrak{a}$ außerhalb der Schar S erzeugt wird. Den Beweis, daß zu jeder (von S^x verschiedenen) isolierten Schar genau ein i. K.-I. gehört, führen wir unter Berufung auf das Endlichkeitsaxiom und die im Anschluß an Hilfssatz 2 gemachte Bemerkung, indem wir zeigen:

Gehört das i. K.-I. $\mathfrak{i}_\mathfrak{b}$ zur Schar S, so sind entweder die höchsten Primideale von $\mathfrak{b}$ mit den höchsten Primidealen von $\mathfrak{a}$ außerhalb S identisch, oder es gibt einen echten Teiler $\mathfrak{b}_1$ von $\mathfrak{b}$, für den $\mathfrak{i}_\mathfrak{b} = \mathfrak{i}_{\mathfrak{b}_1}$ wird. — Es seien $\mathfrak{p}_1', \mathfrak{p}_2', \ldots \mathfrak{p}_s'$ die höchsten Primideale von $\mathfrak{b}$, $\mathfrak{p}_1, \mathfrak{p}_2, \ldots \mathfrak{p}_r$ die höchsten Primideale von $\mathfrak{a}$ außerhalb S. Dann gehört sicher kein $\mathfrak{p}_k'$ der Schar S an, $\mathfrak{p}_i'$ und $\mathfrak{p}_k'$ sind für $i \neq k$ stets gegenseitig prim, und es gibt zu jedem $\mathfrak{p}_i$ mindestens ein $\mathfrak{p}_k' \geqq \mathfrak{p}_i$, weil sicher $\mathfrak{r}' = \mathfrak{p}_1' \cdot \mathfrak{p}_2' \ldots \mathfrak{p}_s' \geqq [\mathfrak{p}_1, \mathfrak{p}_2, \ldots \mathfrak{p}_r]$ ist. Daraus folgt, daß entweder die Primideale $\mathfrak{p}_1', \mathfrak{p}_2' \ldots \mathfrak{p}_s'$ in ihrer Gesamtheit mit $\mathfrak{p}_1, \mathfrak{p}_2, \ldots \mathfrak{p}_r$

7) Auch die überhaupt kein Primideal enthaltende „leere Schar" ist als isolierte Schar anzusehen.

8) Im mengentheoretischen Sinn!

übereinstimmen, oder mindestens ein $\mathfrak{p}_k'$, etwa $\mathfrak{p}_1'$, nicht zu $\mathfrak{a}$ gehört. Im letzteren Fall gibt es ein Ideal $\mathfrak{t} < \mathfrak{p}_1'$ derart, daß $i_\mathfrak{t} = i_{\mathfrak{p}_1'}$ und mithin $i_\mathfrak{b} = i_{\mathfrak{t}'} = i_{\mathfrak{t}\cdot\mathfrak{p}_2'\ldots\mathfrak{p}_s'}$ wird [9]). Es ist daher auch für $\mathfrak{b}_1 = (\mathfrak{b}, \mathfrak{t}\cdot\mathfrak{p}_2' \ldots \mathfrak{p}_s')$: $i_\mathfrak{b} = i_{\mathfrak{b}_1}$ und hier ist $\mathfrak{b}_1$ ein echter Teiler von $\mathfrak{b}$, weil durch $\mathfrak{p}_1'$ unteilbar.

Satz 6 zeigt nicht nur, daß es nur endlich viele i. K.-I. von $\mathfrak{a}$ gibt, sondern er liefert auch eine Möglichkeit, dieselben mit Hilfe der zugehörigen Primideale zu bestimmen.

Definition. Ein Ideal heißt primär, wenn es nur ein einziges zugehöriges Primideal besitzt.

Satz 7. Ein Ideal $\mathfrak{q}$ ist dann und nur dann primär, wenn aus $\mathfrak{a}_1\cdot\mathfrak{a}_2 \geqq \mathfrak{q}$ entweder $\mathfrak{a}_1 \geqq \mathfrak{q}$ oder $\mathfrak{a}_2 \geqq \mathfrak{q}$ oder für genügend großes r: $\mathfrak{a}_1^r \geqq \mathfrak{q}$, $\mathfrak{a}_2^r \geqq \mathfrak{q}$ folgt.

In der Tat, gehört zu $\mathfrak{q}$ nur das Primideal $\mathfrak{p}$, und ist $\mathfrak{a}_1\cdot\mathfrak{a}_2 \geqq \mathfrak{p}$, so ist entweder $(\mathfrak{a}_1, \mathfrak{a}_2) \geqq \mathfrak{p}$, und dann haben wir nach Hilfssatz 2 für genügend großes r: $\mathfrak{a}_1^r \geqq \mathfrak{q}, \mathfrak{a}_2^r \geqq \mathfrak{q}$; oder, es ist etwa $(\mathfrak{a}_2, \mathfrak{p}) < \mathfrak{p}$, dann ist $\mathfrak{q} : \mathfrak{a}_2 = \mathfrak{q}$, mithin $\mathfrak{a}_1 \geqq \mathfrak{q}$. Gehören umgekehrt zu $\mathfrak{q}$ mindestens 2 Primideale $\mathfrak{p}_1$ und $\mathfrak{p}$, und ist etwa $(\mathfrak{p}_1, \mathfrak{p}) < \mathfrak{p}_1$, so haben wir für genügend großes r: $i_\mathfrak{p}^{(\mathfrak{q})}\cdot\mathfrak{p}^r \geqq \mathfrak{q}$, und hier ist weder $i_\mathfrak{p}^{(\mathfrak{q})}$ noch irgend eine Potenz von $\mathfrak{p}^r$ durch $\mathfrak{q}$ teilbar.

§ 4. I. K.-I. und zugehörige Primideale des Produktes und kleinsten gemeinschaftlichen Vielfachen.

Die Untersuchungen von § 3 stützten sich auf Satz 4, in dem die zugehörigen Primideale des Quotienten untersucht wurden. Um zu weiteren Resultaten zu gelangen, studieren wir die Verhältnisse beim Produkt und kleinsten gemeinschaftlichen Vielfachen.

Satz 8. Sind $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{d}$ bel. Ideale, so ist $i_\mathfrak{d}^{(\mathfrak{a}\cdot\mathfrak{b})}$ gleich dem durch $\mathfrak{d}$ erzeugten i. K.-I. von $i_\mathfrak{d}^{(\mathfrak{a})}\cdot i_\mathfrak{d}^{(\mathfrak{b})}$.

Bezeichnen wir der bequemen Schreibweise halber das durch $\mathfrak{d}$ erzeugte i. K.-I. von $i_\mathfrak{d}^{(\mathfrak{a})}\cdot i_\mathfrak{d}^{(\mathfrak{b})}$ mit $i_\mathfrak{d}$, so ist wegen $i_\mathfrak{d}^{(\mathfrak{a})}\cdot i_\mathfrak{d}^{(\mathfrak{b})} \leqq \mathfrak{a}\cdot\mathfrak{b}$ sicher $i_\mathfrak{d} \leqq i_\mathfrak{d}^{(\mathfrak{a}\cdot\mathfrak{b})}$. Wählen wir ferner r hinreichend groß, so wird $i_\mathfrak{d}^{(\mathfrak{a}\cdot\mathfrak{b})} = (\mathfrak{a}\cdot\mathfrak{b}) : \mathfrak{d}^{3r}$; $i_\mathfrak{d} = [(\mathfrak{a} : \mathfrak{d}^r)\cdot(\mathfrak{b} : \mathfrak{d}^r)] : \mathfrak{d}^r$:

9) Dies gilt auch für $\mathfrak{a} : \mathfrak{p}_1' = \mathfrak{a}$, denn dann kann $\mathfrak{p}_1'$ durch das Ideal $\mathfrak{o}$ ersetzt werden, und es ist dabei sicher $\mathfrak{p}_1' > \mathfrak{o}$.

nun ist aber $(\mathfrak{a} : \mathfrak{b}^r) \cdot (\mathfrak{b} : \mathfrak{b}^r) \geqq (\mathfrak{a} \cdot \mathfrak{b}) : \mathfrak{b}^{2r}$ und mithin muß $i_\mathfrak{b} \geqq i_\mathfrak{b}^{(\mathfrak{a} \cdot \mathfrak{b})}$ sein. — Ist etwa $i_\mathfrak{b}^{(\mathfrak{b})} = \mathfrak{o}$, so kann man in dem gegebenen Beweise $i_\mathfrak{b}$ durch $i_\mathfrak{b}^{(\mathfrak{a})}$ ersetzen. Daraus folgt die Formel:

$$i_\mathfrak{a}^{(\mathfrak{a} \cdot \mathfrak{b})} = i_\mathfrak{a}^{(\mathfrak{b})}; \quad i_\mathfrak{b}^{(\mathfrak{a} \cdot \mathfrak{b})} = i_\mathfrak{b}^{(\mathfrak{a})}. \tag{9}$$

Aus Formel (9) ergibt sich weiter:

Gehört $\mathfrak{p}$ zu $\mathfrak{a} \cdot \mathfrak{b}$, so gehört es entweder zu $\mathfrak{a}$ oder zu $\mathfrak{b}$, oder es ist $(\mathfrak{a}, \mathfrak{b}) \geqq \mathfrak{p}$.

In der Tat, ist etwa $(\mathfrak{b}, \mathfrak{p}) < \mathfrak{p}$, so gehört $\mathfrak{p}$ sicher zu $i_\mathfrak{b}^{(\mathfrak{a} \cdot \mathfrak{b})} = i_\mathfrak{b}^{(\mathfrak{a})}$ und mithin zu $\mathfrak{a}$.

Wir können schließlich noch die höchsten, zu $\mathfrak{a}$ $\mathfrak{b}$ gehörigen Primideale bestimmen:

Das Ideal $\mathfrak{p}$ ist dann und nur dann höchstes Primideal von $\mathfrak{a} \cdot \mathfrak{b}$, wenn $\mathfrak{p}$ zu $\mathfrak{a}$ oder $\mathfrak{b}$ gehört, und wenn es kein zu $\mathfrak{a}$ oder $\mathfrak{b}$ gehöriges $\mathfrak{p}' > \mathfrak{p}$ gibt.

Zum Beweise bezeichne man mit $\mathfrak{r}$ das Produkt aller entweder zu $\mathfrak{a}$, oder zu $\mathfrak{b}$ oder zu $\mathfrak{a} \cdot \mathfrak{b}$ gehöriger, nicht durch $\mathfrak{p}$ teilbarer Primideale, bilde dann $i_\mathfrak{r}^{(\mathfrak{a} \cdot \mathfrak{b})}$, $i_\mathfrak{r}^{(\mathfrak{a})}$, $i_\mathfrak{r}^{(\mathfrak{b})}$ und beachte Satz 5 sowie Satz 8 nebst Folgerungen! Die gewonnenen Ergebnisse stellen, wie durch Beispiele gezeigt werden kann, im gewissen Sinne das Maximum dar, was sich über die i. K.-I. und die zugehörigen Primideale des Produktes aussagen läßt.

Für die i K.-I. des kleinsten gemeinschaftlichen Vielfachen gilt die unmittelbar aus dem distributiven Gesetz der Division folgende Formel:

$$i_\mathfrak{b}^{([\mathfrak{a}_1, \mathfrak{a}_2, \ldots \mathfrak{a}_n])} = [i_\mathfrak{b}^{(\mathfrak{a}_1)}, i_\mathfrak{b}^{(\mathfrak{a}_2)}, \ldots i_\mathfrak{b}^{(\mathfrak{a}_n)}]. \tag{10}$$

Ferner ist leicht zu sehen, daß zu $[\mathfrak{a}_1, \mathfrak{a}_2 \ldots \mathfrak{a}_n]$ nur solche Primideale gehören können, die auch zu einem der Ideale $\mathfrak{a}_i$ gehören.

In der Tat, bedeutet $\mathfrak{r}$ das Produkt aller entweder zu $\mathfrak{a} = [\mathfrak{a}_1, \mathfrak{a}_2 \ldots \mathfrak{a}_n]$ oder zu einem der $\mathfrak{a}_i$ gehörigen, nicht durch $\mathfrak{p}$ teilbaren Primideale, so bilde man $i_\mathfrak{r}^{(\mathfrak{a})} = [i_\mathfrak{r}^{(\mathfrak{a}_1)}, i_\mathfrak{r}^{(\mathfrak{a}_2)}, \ldots i_\mathfrak{r}^{(\mathfrak{a}_n)}]$[10]. Hier sind die Primideale von $i_\mathfrak{r}^{(\mathfrak{a}_i)}$ sämtlich Vielfache von $\mathfrak{p}$. Gehört nun $\mathfrak{p}$ zu $\mathfrak{a}$, so wird $i_\mathfrak{r}^{(\mathfrak{a})} : \mathfrak{p} = [i_\mathfrak{r}^{(\mathfrak{a}_1)} : \mathfrak{p}, i_\mathfrak{r}^{(\mathfrak{a}_2)} : \mathfrak{p}, \ldots i_\mathfrak{r}^{(\mathfrak{a}_n)} : \mathfrak{p}] < i_\mathfrak{r}^{(\mathfrak{a})}$. Es muß daher für mindestens ein i der Quotient $i_\mathfrak{r}^{(\mathfrak{a}_i)} : \mathfrak{p} < i_\mathfrak{r}^{(\mathfrak{a}_i)}$ werden, und das ist nur möglich, wenn $\mathfrak{p}$ zu $i_\mathfrak{r}^{(\mathfrak{a}_i)}$ und mithin zu $\mathfrak{a}_i$ gehört.

10) Ist $i_\mathfrak{r}^{(\mathfrak{a}_i)} = \mathfrak{o}$, so ist diese Komponente wegzulassen!

Aus dem gewonnenen Resultat folgt insbesondere, daß das kleinste gemeinschaftliche Vielfache zweier zum gleichen Primideal gehöriger Primärideale selbst primär ist, und dasselbe zugehörige Primideal besitzt wie die Komponenten. Ferner haben wir:

Satz 9. Ist $\mathfrak{a} = [\mathfrak{q}_1, \mathfrak{q}_2, \ldots \mathfrak{q}_n]$ eine Darstellung von $\mathfrak{a}$ durch Primärideale, bei der keine Komponente überflüssig ist, und gehört zu $\mathfrak{q}_i$ das Primideal $\mathfrak{p}_i$, so gehören zu $\mathfrak{a}$ gerade die Primideale $\mathfrak{p}_1, \mathfrak{p}_2, \ldots \mathfrak{p}_n$.

Beim Beweise dürfen wir voraussetzen, daß alle $\mathfrak{p}_i$ verschieden sind, weil man sonst zwei Primärkomponenten einfach zu einem neuen Primärideal mit gleichem zugehörigem Primideal zusammenfassen könnte. Um nun zu zeigen, daß $\mathfrak{p}_i$ zu $\mathfrak{a}$ gehören muß, denke man sich die $\mathfrak{q}_i$ so numeriert, daß $\mathfrak{p}_k > \mathfrak{p}_i$ $(k < i)$; $(\mathfrak{p}_i, \mathfrak{p}_k) < \mathfrak{p}_i$ $(k > i)$ ist, und bilde mit $\mathfrak{r} = \mathfrak{q}_{i+1} \cdot \mathfrak{q}_{i+2} \ldots \mathfrak{q}_n$ die Ideale $\mathfrak{i}_r^{(a)} = [\mathfrak{q}_1, \mathfrak{q}_2, \ldots \mathfrak{q}_i]$; $\mathfrak{i}_r^{(a)} : \mathfrak{q}_i = [\mathfrak{q}_1, \mathfrak{q}_2, \ldots \mathfrak{q}_{i-1}]$. Wenn nun $\mathfrak{p}_i$ nicht zu $\mathfrak{a}$ gehörte, so wäre $\mathfrak{i}_r^{(a)} : \mathfrak{q}_i = \mathfrak{i}_r^{(a)}$, d. h. $[\mathfrak{q}_1, \mathfrak{q}_2, \ldots \mathfrak{q}_{i-1}] = [\mathfrak{q}_1, \mathfrak{q}_2 \ldots \mathfrak{q}_i]$; $\mathfrak{a} = [\mathfrak{q}_1, \mathfrak{q}_2, \ldots \mathfrak{q}_{i-1}, \mathfrak{q}_{i+1}, \ldots \mathfrak{q}_n]$ entgegen der Vor., daß kein $\mathfrak{q}_i$ in der Darstellung von $\mathfrak{a}$ überflüssig ist.

Satz 10. Sind $\mathfrak{i}_1$ und $\mathfrak{i}_2$ zwei i. K.-I. von $\mathfrak{a}$, die zu den isolierten Scharen S_1 und S_2 gehören, so ist $[\mathfrak{i}_1, \mathfrak{i}_2]$ dasjenige i. K.-I. von $\mathfrak{a}$, das zur Vereinigungsschar S von S_1 und S_2 gehört.

Ist etwa $\mathfrak{i}_1 = \mathfrak{a}$, so ist die Behauptung trivial; ist aber $\mathfrak{i}_1 < \mathfrak{a}$; $\mathfrak{i}_2 < \mathfrak{a}$, so existieren zwei Ideale $\mathfrak{b}_1$ und $\mathfrak{b}_2$ derart, daß $\mathfrak{i}_1 = \mathfrak{i}_{\mathfrak{b}_1}$; $\mathfrak{i}_2 = \mathfrak{i}_{\mathfrak{b}_2}$ wird. Dann ist nach Formel (7) sicher $[\mathfrak{i}_1, \mathfrak{i}_2] = \mathfrak{i}_{(\mathfrak{b}_1, \mathfrak{b}_2)}$, und aus Satz 5 folgt, daß $(\mathfrak{b}_1, \mathfrak{b}_2)$ durch alle und nur die Primideale von $\mathfrak{a}$ teilbar ist, die nicht in der Schar S vorkommen.

§ 5. Darstellungen von $\mathfrak{a}$ als kleinstes gemeinschaftliches Vielfaches von i. K.-I.

Unter einer „Darstellung von $\mathfrak{a}$" soll in diesem Paragraphen stets eine kleinste-gemeinschaftliche-Vielfachen-Darstellung verstanden werden.

Definition. Eine Darstellung von $\mathfrak{a}$ durch i. K.-I. heißt „isoliert irreduzibel", wenn keine Komponente

weggelassen oder durch einen echten Teiler, der gleichfalls i. K.-I. von $\mathfrak{a}$ ist, ersetzt werden kann.

Ein Ideal heißt isoliert irreduzibel, wenn es keine Darstellung $\mathfrak{a} = [\mathfrak{i}_1^{(\mathfrak{a})}, \mathfrak{i}_2^{(\mathfrak{a})}]$, $\mathfrak{i}_1^{(\mathfrak{a})} < \mathfrak{a}$, $\mathfrak{i}_2^{(\mathfrak{a})} < \mathfrak{a}$ gibt.

Definition. Ist $\mathfrak{p}$ ein niederstes Primideal von $\mathfrak{a}$, so verstehen wir unter der „durch $\mathfrak{p}$ bestimmten Hauptkomponente $\mathfrak{g}$" dasjenige i. K.-I. von $\mathfrak{a}$, das zu der Schar aller durch $\mathfrak{p}$ teilbaren Primideale[11]) von $\mathfrak{a}$ gehört.

Satz 11. Sind $\mathfrak{p}_i$ die niedersten Primideale von $\mathfrak{a}$, $\mathfrak{g}_i$ die zugehörigen Hauptkomponenten ($i = 1, 2 \ldots n$), so ist $\mathfrak{a} = [\mathfrak{g}_1, \mathfrak{g}_2, \ldots \mathfrak{g}_n]$.

Ein Ideal ist dann und nur dann isoliert irreduzibel, wenn es nur ein einziges niederstes Primideal besitzt.

Die Behauptungen ergeben sich mühelos als Korollar zu Satz 10.

Wir wollen die Darstellung $\mathfrak{a} = [\mathfrak{g}_1, \mathfrak{g}_2, \ldots \mathfrak{g}_n]$ als „Hauptdarstellung von $\mathfrak{a}$" bezeichnen. Dann gilt:

Satz 12. Jede isoliert reduzierte Darstellung von $\mathfrak{a}$ entsteht aus der Hauptdarstellung durch gruppenweise Zusammenfassung der Komponenten[12]).

Es seien wie oben $\mathfrak{p}_1, \mathfrak{p}_2, \ldots \mathfrak{p}_n$ die niedersten Primideale von $\mathfrak{a}$, $\mathfrak{a} = [\mathfrak{i}_1, \mathfrak{i}_2, \ldots \mathfrak{i}_m]$ sei die gegebene isoliert reduzierte Darstellung. Dann folgt aus Satz 10, daß es zu jedem $\mathfrak{p}_k$ ein $\mathfrak{i}_l$ geben muß, derart, daß $\mathfrak{p}_k$ zu $\mathfrak{i}_l$ gehört. Ferner ist aus Satz 10 zu schließen, daß diejenigen $\mathfrak{i}_l$, zu denen überhaupt kein $\mathfrak{p}_k$ gehört, in der Darstellung $\mathfrak{a} = [\mathfrak{i}_1, \mathfrak{i}_2, \ldots \mathfrak{i}_m]$ überflüssig sind, daß also solche Komponenten bei einer isoliert reduzierten Darstellung überhaupt nicht auftreten. Es mögen nun etwa $\mathfrak{p}_{k_1}, \mathfrak{p}_{k_2}, \ldots \mathfrak{p}_{k_{l_k}}$ zu $\mathfrak{i}_k$ gehören ($k = 1, 2 \ldots m$). Dann ist $\mathfrak{i}_k \geqq [\mathfrak{g}_{k_1}, \mathfrak{g}_{k_2}, \ldots \mathfrak{g}_{k_{l_k}}]$ und $\mathfrak{a} = [\ldots [\mathfrak{g}_{k_1}, \mathfrak{g}_{k_2}, \ldots \mathfrak{g}_{k_{l_k}}] \ldots]$. Da die Darstellung durch die $\mathfrak{i}_k$ nach Vor. isoliert reduziert ist, folgt daraus: $\mathfrak{i}_k = [\mathfrak{g}_{k_1}, \mathfrak{g}_{k_2}, \ldots \mathfrak{g}_{k_{l_k}}]$. Schließlich kann es nicht

---

11) $\mathfrak{p}$ eingeschlossen!

12) Dabei darf keine der Hauptkomponenten in zwei verschiedene Gruppen hineingenommen werden!

vorkommen, daß für $l \neq k$ etwa $g_{l_i} = g_{k_i}$ wird. Denn andernfalls könnte man z. B. i_k durch den echten Teiler $[g_{k_2}, g_{k_3}, \ldots g_{k_{l_k}}]$ ersetzen.

Als Anwendung des gewonnenen Resultates beweisen wir:

Satz 13. Jede Darstellung von a durch gegenseitig prime Komponenten ist isoliert reduziert, und entsteht daher aus der Hauptdarstellung durch gruppenweise Zusammenfassung der Komponenten[13]).

In der Tat, ist $a = [a_1, a_2, \ldots a_m]$; $a_i : a_k = a_i$ $[i \neq k]$, und setzen wir $b_k = \prod_{k \neq l} a_i$, so ist $a_k = i_{b_k}^{(a)}$; ist ferner $a = [a_1, a_2, \ldots a_m] = [a_1', a_2, \ldots a_m]$, so ist $a : b_1 = a_1 = a_1' : b_1$, also sicher $a_1 \equiv a_1'$, es kann mithin in der Darstellung von a kein a_i durch einen echten Teiler ersetzt werden.

§ 6. Teilerfremde Ideale.

Genügt ein Ideal e der Gleichung $a \cdot e = a$ für beliebiges a, so folgt aus $o \cdot e = o \geq e$ notwendig $e = o$.

Definition. Ist $a \cdot o = a$ für beliebiges a, so heißen a und b teilerfremd, wenn $(a, b) = o$ ist.

Für teilerfremde Ideale gelten folgende Formeln:

$$a : b = a, \quad b : a = b, \quad \text{wenn } (a, b) = o. \tag{11}$$

Ist nämlich etwa $b \cdot b \geq a$, so ist auch $b \cdot (b, a) = b \cdot o = b \geq a$.

$$(\prod_{i=1}^{r} a_i, \prod_{k=1}^{s} b_k) = o, \text{ wenn } (a_i, b_k) = o \tag{12}$$

Für hinreichend großes t wird nämlich $\prod_{i,k} (a_i, b_k)^t = o^{r \cdot s \cdot t} = o \geq (\prod_i a_i, \prod_k b_k)$.

$$[a_1, a_2, \ldots a_n] = a_1 \cdot a_2 \ldots a_n, \text{ wenn } (a_i, a_k) = o \ (i \neq k). \tag{13}$$

Man setze $a^{(i)} = \prod_{k \neq l} a_k$. Dann wird, wie leicht zu sehen, $(a^{(1)}, a^{(2)}, \ldots a^{(n)}) = o$, und man hat $a_1 \cdot a_2 \ldots a_n \leq [a_1, a_2, \ldots a_n]$

13) Über Darstellungen durch gegenseitig prime Komponenten vgl. N. § 6 p. 47 f., wo insbesondere eine eindeutig bestimmte Darstellung durch „kleinste" gegenseitig prime Ideale konstruiert wird, aus der alle anderen derartigen Darstellungen durch gruppenweise Zusammenfassung der Komponenten entstehen.

$\cdot(\mathfrak{a}^{(1)}, \mathfrak{a}^{(2)}, \ldots \mathfrak{a}^{(n)}) = [\mathfrak{a}_1, \mathfrak{a}_2, \ldots \mathfrak{a}_n]$, also $\mathfrak{a}_1 \cdot \mathfrak{a}_2 \ldots \mathfrak{a}_n = [\mathfrak{a}_1, \mathfrak{a}_2, \ldots \mathfrak{a}_n]$.

Definition. Besteht eine Gleichung $\mathfrak{a} = \mathfrak{a}_1 \cdot \mathfrak{a}_2$; $\mathfrak{a}_1 < \mathfrak{a}$, $\mathfrak{a}_2 < \mathfrak{a}$; $(\mathfrak{a}_1, \mathfrak{a}_2) = \mathfrak{o}$, so heißt $\mathfrak{a}$ „teilerfremd reduzibel", im andern Falle wird es „teilerfremd irreduzibel" genannt.

Satz 14. Jedes Ideal $\mathfrak{a} > \mathfrak{o}$ läßt sich eindeutig als Produkt teilerfremd irreduzibler von $\mathfrak{o}$ verschiedener Faktoren darstellen.

Die Existenz einer Darstellung der angegebenen Art folgt aus dem Endlichkeitsaxiom. Es seien jetzt $\mathfrak{a} = \mathfrak{a}_1 \cdot \mathfrak{a}_2 \ldots \mathfrak{a}_\sigma = \mathfrak{b}_1 \cdot \mathfrak{b}_2 \ldots \mathfrak{b}_\tau$ zwei derartige Darstellungen, und es sei, was stets möglich ist, die Bezeichnung so gewählt, daß $(\mathfrak{a}_1, \mathfrak{b}_1) \neq \mathfrak{o}$ ist. Setzen wir dann $\mathfrak{c}_i = (\mathfrak{a}_1, \mathfrak{b}_i)$, so wird $(\mathfrak{c}_i, \mathfrak{c}_k) = \mathfrak{o}$ $(i \neq k)$, und wir haben $\prod_{i=1}^{\tau} \mathfrak{c}_i = [\mathfrak{c}_1, \mathfrak{c}_2, \ldots \mathfrak{c}_n] \leqq \mathfrak{a}_1$. Andererseits folgt durch Ausmultiplikation nach dem distributiven Gesetz: $\prod_{i=1}^{\tau} \mathfrak{c}_i \cdot \prod_{k=2}^{\sigma} \mathfrak{a}_k \geqq \mathfrak{a}$, und nach Formel (11) ergibt sich daraus $\prod_{i=1}^{\tau} \mathfrak{c}_i \geqq \mathfrak{a}_1$, also $\prod_{i=1}^{\tau} \mathfrak{c}_i = \mathfrak{a}_1$. Da nun $\mathfrak{a}_1$ nach Vor. teilerfremd irreduzibel und $\mathfrak{c}_1 > \mathfrak{o}$ ist, so haben sicher $\mathfrak{c}_i = \mathfrak{o}$ $(i \geqq 2)$, $\mathfrak{c}_1 = \mathfrak{a}_1$, d. h. $\mathfrak{a}_1 \leqq \mathfrak{b}_1$. In ganz analoger Weise findet man $\mathfrak{b}_1 \leqq \mathfrak{a}_1$, es ist also $\mathfrak{a}_1 = \mathfrak{b}_1$. Aus der Gleichung $\mathfrak{a}_1 \mathfrak{a}_2 \ldots \mathfrak{a}_\sigma = \mathfrak{a}_1 \cdot \mathfrak{b}_2 \ldots \mathfrak{b}_\tau$ erschließen wir mit Hilfe von Formel (11) die Gültigkeit der Gleichung $\mathfrak{a}_2 \cdot \mathfrak{a}_3 \ldots \mathfrak{a}_\sigma = \mathfrak{b}_2 \cdot \mathfrak{b}_3 \ldots \mathfrak{b}_\tau$ und führen dann nach üblichem Schema den Eindeutigkeitsbeweis zu Ende.

Satz 4 hätte auch aus der in § 2—5 entwickelten Theorie mit Hilfe folgender Sätze erschlossen werden können [14]).

---

14) Vgl. N. § 8, wo der im folgenden nur angedeutete Beweis ausführlich entwickelt ist. Ein anderer Beweis von Satz 11, der, wie der im Text durchgeführte, ohne Zuhilfenahme der zugehörigen Primideale und i. K.-I. auskommt, aber dafür die Theorie der für uns nicht definierbaren „Restgruppe nach einem Ideal" verwendet, findet sich bei Noether-Schmeidler, Moduln in nichtkommutativen Bereichen, insbesondere aus Differential- und Differenzenausdrücken, Math. Zeitschrift 8, p. 1—35, § 7.

Ist $\mathfrak{a} = \mathfrak{a}_1 \cdot \mathfrak{a}_2 \ldots \mathfrak{a}_n = [\mathfrak{a}_1, \mathfrak{a}_2, \ldots \mathfrak{a}_n]$; $(\mathfrak{a}_i, \mathfrak{a}_k) = \mathfrak{o}\ (i \neq k)$, so sind die $\mathfrak{a}_i$ i. K.-I. von $\mathfrak{a}$.

(Folgt aus Formel (11) und Satz 13).

Es ist $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}$ dann und nur dann, wenn jedes zu $\mathfrak{a}$ gehörige Primideal zu jedem zu $\mathfrak{b}$ gehörigen Primideal teilerfremd ist.

(Folgt aus Hilfssatz 2 und Formel (12)).

$\mathfrak{a}$ ist dann und nur dann teilerfremd reduzibel, wenn die Schar S der zugehörigen Primideale derart in zwei nicht leere isolierte Teilscharen S_1 und S_2 zerlegt werden kann, daß jedes Primideal aus S_1 zu jedem Primideal aus S_2 teilerfremd ist.

(Folgt aus dem unmittelbar vorangehenden Satz, sowie aus Satz 10).

Mit Hilfe der gewonnenen Resultate kann man leicht zu einem neuen Beweis von Satz 14 gelangen, und darüber hinaus die teilerfremd irreduziblen Faktoren von $\mathfrak{a}$ durch die zu $\mathfrak{a}$ gehörigen Primideale charakterisieren. Demgegenüber hat der oben gegebene Beweis den Vorzug größerer Einfachheit.