Über die Produktzerlegung der Hauptideale. II.

Von

Shinziro MORI.

(Eingegangen am 22. 5. 1939.)

In der vorliegenden zweiten Mitteilung[1] wird statt der Behauptung[2] von Schmidt ein wichtiger Satz bewiesen werden, der die notwendigen und hinreichenden Bedingungen für die Produktzerlegung der Hauptideale eines allgemeinen Integritätsbereiches $\mathfrak{J}$ gibt.

Notwendige Bedingungen.

In diesem Paragraphen sei $\mathfrak{J}$ ein allgemeiner Integritätsbereich mit *Einselement*, in dem jedes Hauptideal sich als Potenzprodukt der

(1) Vgl. die erste Mitteilung: Über die Produktzerlegung der Hauptideale, dieses Jour. **8** (1938), 7.

(2) F. K. Schmidt, Über die Primidealzerlegung der Hauptideale eines Integritätsbereichs, Sitz.-Ber. München. Akad. Wiss. (1928), 285.

Satz von Schmidt. *Damit in einem Integritätsbereich $\mathfrak{J}$ jedes Hauptideal als Potenzprodukt von Primidealen darstellbar ist, ist notwendig und hinreichend dass*

1) *jede mit einem Hauptideal beginnende Idealquotienten-kette im Endlichen abbricht,*

2) *$\mathfrak{J}$ ganz abgeschlossen ist.*

Die Notwendigkeit der Bedingungen folgt leicht aus Sätze 6, 8 und 9, aber die Bedingungen sind durch das folgende Beispiel nicht hinreichend:

Beispiel. Ist C der Ring aller ganzen rationalen Zahlen, so ist der Ring $C[x, \sqrt{2x}]$ ganz abgeschlossen und in diesem Bereich ist die erste Bedingung auch erfüllt. Das Hauptideal (x) ist aber als ein Potenzprodukt der Primideal nicht darstellbar, da (x) ein zum Primideal $(x, \sqrt{2x})$ gehöriges Primärideal ist. (B. L. van der Waerden, *Moderne Algebra* II, 108.)

Ist $\mathfrak{J}$ ein Integritätsbereich mit Teilerkettensatz, so ergibt sich der folgende Satz:

Notwendig und hinreichend, damit $\mathfrak{J}$ ganz abgeschlossen sei, ist, dass kein Primärideal zwischen den symbolischen Potenzen $\mathfrak{p}^{(1)}$ und $\mathfrak{p}^{(2)}$ des zu einem beliebigen Hauptideal gehörigen Primideals $\mathfrak{p}$ je eingeschaltet werden kann.

Der Beweis dieses Satzes beruht auf der Bewertungstheorie (W. Krull, *Idealtheorie*, 100) und auch ohne Benutzung dieser Theorie können wir den Satz beweisen (S. Mori, Bedingungen für ganze Abgeschlossenheit in Integritätsbereichen, dieses Jour. **7** (1937), 15).

endlich vielen Primideale darstellen lässt. Um die gewünschten notwendigen Bedingungen zu gewinnen, müssen wir zuerst den wichtigen Satz vorausschicken.

Satz 8. *Lässt jedes Hauptideal in $\mathfrak{J}$ sich als Potenzprodukt der endlich vielen Primideale darstellen, so müssen alle Primideale in dieser Produkt-darstellung ein in $\mathfrak{J}$ minimales Primideal sein.*[1]

Durch Verbindung dieses Satzes mit den in der ersten Mitteilung gewonnenen Sätzen 4 und 5 ergibt sich also:

Satz 9. *Ist (a) ein beliebiges Hauptideals aus $\mathfrak{J}$, so bricht die Idealquotienten-kette $(a):\mathfrak{a}_1 \subset (a):\mathfrak{a}_2 \subset (a):\mathfrak{a}_3 \subset \cdots$ stets im Endlichen ab.*

Nach unserer Voraussetzung für $\mathfrak{J}$ ist

$$(a) = \mathfrak{p}_1^{k_1}\mathfrak{p}_2^{k_2}\ldots\ldots\mathfrak{p}_m^{k_m},$$

wobei $\mathfrak{p}_i$ aber nach Satz 8 ein in $\mathfrak{J}$ minimales Primideal bedeutet. Da nach Satz 5 jede Potenz von $\mathfrak{p}_i$ primär ist, so muss $\mathfrak{a}_j$ dann und nur dann durch wenigstens eines aus $\mathfrak{p}_i$ $(i=1,2,\ldots\ldots,m)$ teilbar sein, wenn $(a):\mathfrak{a}_j$ von (a) verschieden ist, und ferner muss $\mathfrak{a}_j$ dann und nur dann durch jedes $\mathfrak{p}_i^{k_i}$ teilbar, oder $\mathfrak{a}_j \equiv 0\ (a)$ sein, wenn $(a):\mathfrak{a}_j = \mathfrak{J}$ ist. Ist $(a):\mathfrak{a}_j$ von $\mathfrak{J}$ und (a) verschieden, so muss damit nach Satz 4 $\mathfrak{a}_j \equiv 0\ (\mathfrak{p}_i^{s_i})$, $\not\equiv 0\ (\mathfrak{p}_i^{s_i+1})$ $(i=1,2,\ldots\ldots,m)$ sein,[2] wobei wenigstens eines aus s_i $(i=1,2,\ldots\ldots,m)$ von Null verschieden und auch wenigstens eines aus s_i kleiner als k_i sein muss. Wenn für dieselben s_i $\mathfrak{a}_{j+1} \equiv 0\ (\mathfrak{p}_i^{s_i})$, $\not\equiv 0\ (\mathfrak{p}_i^{s_i+1})$ $(i=1,2,\ldots\ldots,m)$ ist, so wird $(a):\mathfrak{a}_j = (a):\mathfrak{a}_{j+1}$. Sonst würde $a'\mathfrak{a}_j \not\equiv 0\ (a)$, $a'\mathfrak{a}_{j+1} \equiv 0\ (a)$ für ein Element a' und aus $a'\mathfrak{a}_{j+1} \equiv 0\ (a)$ folgte $a' \equiv 0\ (\mathfrak{p}_i^{k_i - s_i})$ für $k_i - s_i > 0$. Da aber wenigstens eines aus $k_i - s_i$ $(i=1,2,\ldots\ldots,m)$ positiv sein muss, hätten wir danach einen Widerspruch zu $a'\mathfrak{a}_j \not\equiv 0\ (a)$. Ist $\mathfrak{a}_{j+1} \equiv 0\ (\mathfrak{p}_i^{s_i'})$, $\not\equiv 0\ (\mathfrak{p}_i^{s_i'+1})$ $(i=1,2,\ldots\ldots,m)$ und ist $k_i \geqq s_i > s_i'$ für ein s_i', so muss $(a):\mathfrak{a}_j$ durch $(a):\mathfrak{a}_{j+1}$ unteilbar sein. Denn wir können ein Element a_i finden, so dass $a_i \equiv 0\ (\mathfrak{p}_i^{k_i - s_i'})$, $\not\equiv 0\ (\mathfrak{p}_i^{k_i - s_i'})$, $a_i \equiv 0\ (\mathfrak{p}_1^{k_1}\ldots\mathfrak{p}_{i-1}^{k_{i-1}}\mathfrak{p}_{i+1}^{k_{i+1}}\ldots\mathfrak{p}_m^{k_m})$ ist. Dann ist $(a_i) \equiv 0\ \big((a):\mathfrak{a}_j\big)$, $\not\equiv 0\ \big((a):\mathfrak{a}_{j+1}\big)$ und folglich ist $(a):\mathfrak{a}_j$ durch $(a):\mathfrak{a}_{j+1}$ unteilbar. Dafür,

(1) S. Mori, Zerlegung der Hauptideale aus Polynomringen in minimale Primideale. II, dieses Jour. **9** (1939), 5.

(2) Für ein von Null verschiedenes Element a_j aus $\mathfrak{a}_j$ ist $(a_j) = \mathfrak{p}_1^{s_1}\mathfrak{p}_2^{s_2}\ldots\ldots$ und nach Satz 4 ist $\mathfrak{p}_i^n \neq \mathfrak{p}_i^{n+1}$ für jedes n. Hiermit muss s_i eine endliche ganze rationale Zahl sein.

dass $(a):\mathfrak{a}_j \subset (a):\mathfrak{a}_{j+1}$ gültig ist, muss damit $s_i < s_i' \leqq k_i$ für wenigstens ein s_i und $s_l \leqq s_l' \leqq k_l$ oder $k_l \leqq s_l$, $k_l \leqq s_l'$ für jedes andere s_l sein. Indem wir so fortfahren, erhalten wir schliesslich, dass $\mathfrak{a}_n \equiv 0\ (a)$ ist, und die Idealquotienten-kette $(a):\mathfrak{a}_1 \subset (a):\mathfrak{a}_2 \subset \cdots$ muss im Endlichen abbrechen.

Durch Einführung des umkehrbaren,[1] in $\mathfrak{J}$ minimalen Primideals ergibt sich eine notwendige Bedingung auch:

Satz 10. *Jedes höchste Primideal eines beliebigen Hauptideals aus $\mathfrak{J}$ ist umkehrbar.*

Ist (a) ein beliebiges Hauptideal in $\mathfrak{J}$, so ist $(a)=\mathfrak{p}_1^{k_1}\mathfrak{p}_2^{k_2}\ldots\mathfrak{p}_m^{k_m}$ und nach Satz 8 ist jedes $\mathfrak{p}_i$ ein in $\mathfrak{J}$ minimales Primideal und folglich ist ein höchstes Primideal $\mathfrak{p}$ von (a) mit einem aus $\mathfrak{p}_i$ $(i=1,2,\ldots,m)$ identisch, also ein in $\mathfrak{J}$ minimales Primideal. Da aber nach Satz 4 $\mathfrak{p} \neq \mathfrak{p}^2$ ist, können wir ein Element p auswählen, so dass $p \equiv 0\ (\mathfrak{p})$, $\not\equiv 0\ (\mathfrak{p}^2)$ ist. Dann ist nach unserer Voraussetzung über $\mathfrak{J}$ $(p)=\mathfrak{p}\mathfrak{p}_1'^{k_1}\ldots\mathfrak{p}_l'^{k_l}$. Wenn $(p)=\mathfrak{p}$ ist, so ist $\mathfrak{p}$ offenbar umkehrbar. Damit nehmen wir $(p) \neq \mathfrak{p}$ an und danach existiert ein von Null verschiedenes Element r in $\mathfrak{p}_1'^{k_1}\ldots\mathfrak{p}_l'^{k_l}$. Für das Element r gilt $\mathfrak{p}(r) \equiv 0\ (p)$. Daher können wir $\mathfrak{p}(r)=\mathfrak{a}(p)$, $(r)=\mathfrak{p}_1'^{k_1}\ldots\mathfrak{p}_l'^{k_l}\mathfrak{p}_1''^{k_1''}\ldots$ setzen, wobei es möglich ist, dass ein $\mathfrak{p}''$ mit einem $\mathfrak{p}'$ identisch ist. Ist nun r' ein anderes beliebiges Element aus $\mathfrak{p}_1'^{k_1}\mathfrak{p}_2'^{k_2}\ldots\mathfrak{p}_l'^{k_l}$, so können wir auch $\mathfrak{p}(r')=\mathfrak{a}'(p)$ setzen, und auf diese Weise entspricht ein Ideal $\mathfrak{a}$ einem beliebigen Element aus $\mathfrak{p}_1'^{k_1}\mathfrak{p}_2'^{k_2}\ldots\mathfrak{p}_l'^{k_l}$. Es sei nun $\mathfrak{v}$ die Summe aller zu r entsprechenden Ideale $\mathfrak{a}$, dann erhalten wir $(p)=\mathfrak{p}\mathfrak{p}_1'^{k_1}\ldots\mathfrak{p}_l'^{k_l}=\mathfrak{v}(p)$. Also ist.

$$\mathfrak{v}=\mathfrak{J}. \tag{1}$$

Ist $\mathfrak{R}$ der Quotientenkörper von $\mathfrak{J}$, so gehört das Element $\frac{r}{p}$ aus $\mathfrak{R}$ zu $\mathfrak{p}^{-1}$, und daher folgt nach (1) $\mathfrak{p}\mathfrak{p}^{-1}=\mathfrak{J}$. Also ist jedes höchste Primideal von (a) umkehrbar.

Hinreichende Bedingungen.

Zunächst nehmen wir im allgemeinen Integritätsbereich $\mathfrak{J}$ mit Einselement die Gültigkeit der folgenden Bedingung an:

(1) W. Krull, *Idealtheorie*, 13. Ein ideal $\mathfrak{a}$ heisst „*umkehrbar*, wenn $\mathfrak{a}\mathfrak{a}^{-1}=\mathfrak{J}$ ist. B. L. van der Waerden, *Moderne Algebra* I, 47. Jeder Integritätsbereich lässt sich in einen Körper einbetten.

Bedingung I. *Ist* (a) *ein beliebiges Hauptideal in* $\mathfrak{J}$, *so bricht die Idealquotienten-kette*

$$(a):\mathfrak{a}_1 \subset (a):\mathfrak{a}_2 \subset \cdots \subset (a):\mathfrak{a}_n \subset \cdots$$

stets im Endlichen ab.

Es gilt dann der

Satz 11. *Jedes Hauptideal* (a) *in* $\mathfrak{J}$ *besitzt ein zu ihm gehöriges höchstes Primideal* (*minimales Primoberideal*),[1] *wenn in* $\mathfrak{J}$ *Bedingung I erfüllt ist.*

Es sei $\mathfrak{h}$ das zu (a) gehörige Halbprimideal und es sei r' ein durch $\mathfrak{h}$ unteilbares Element. Dann ist jede Potenz von r' durch $\mathfrak{h}$ unteilbar und nach Bedingung I bricht die Idealquotienten-kette $(a):(r') \subset (a):(r'^2) \subset \cdots$ im Endlichen ab. Wenn für eine hinreichend grosse ganze Zahl n_1 wir $r_1 = r'^{n_1}$ setzen, so erhalten wir danach

$$(1) \qquad \mathfrak{q}_1 = (a):(r_1) = (a):(r_1^2) = \cdots, \quad r_1 \not\equiv 0 \ (\mathfrak{h}), \ \not\equiv 0 \ (\mathfrak{q}_1).$$

Es sei $\mathfrak{h}_1$ auch das zu $\mathfrak{q}_1$ gehörige Halbprimideal. Dann ist $r_1 \not\equiv 0 \ (\mathfrak{h}_1)$ nach (1). Ist $\mathfrak{h}_1$ kein Primideal, so können wir zwei verschiedene Elemente r_1' und r_1'' auswählen, so dass $r_1' r_1'' \equiv 0 \ (\mathfrak{h}_1)$, $r_1' \not\equiv 0 \ (\mathfrak{h}_1)$, $r_1'' \not\equiv 0 \ (\mathfrak{h}_1)$ ist, und auch bricht die Idealquotienten-kette $(a):(r_1) \subset (a):(r_1 r_1') \subset (a):(r_1 r_1')^2 \subset \cdots$ im Endlichen ab. Setzen wir $r_2 = (r_1 r_1')^{n_2}$ für eine hinreichend grosse Zahl n_2, so erhalten wir wieder

$$(2) \qquad \mathfrak{q}_2 = (a):(r_2) = (a):(r_2^2) = \cdots, \quad r_2 \not\equiv 0 \ (\mathfrak{q}_2), \ r_2 \not\equiv 0 \ (\mathfrak{h}_1).$$

Nach $r_1'' \not\equiv 0 \ (\mathfrak{h}_1)$ ist jede Potenz von r_1'' durch $\mathfrak{q}_1$ unteilbar. Aber aus $r_1' r_2'' \equiv 0 \ (\mathfrak{h}_1)$ folgt nach (1) $(r_1' r_1'')^k r_1 \equiv 0 \ (a)$ für eine genügend grosse Zahl k und daher ergibt sich nach (2) leicht $r_1''^k \equiv 0 \ (\mathfrak{q}_2)$. Also gilt $\mathfrak{q}_1 \subset \mathfrak{q}_2$ denn aus $q_1 r_1 \equiv 0 \ (a)$ folgt $q_1 (r_1 r_1')^{n_2} \equiv 0 \ (a)$, oder $q_1 r_2 \equiv 0 \ (a)$. Ist das zu $\mathfrak{q}_2$ gehörige Halbprimideal $\mathfrak{h}_2$ wieder nicht prim, so erhalten wir auf genau dieselben Weise die Kette von Idealquotienten $\mathfrak{q}_1 \subset \mathfrak{q}_2 \subset \mathfrak{q}_3 = (a):(r_3) = (a):(r_3^2) = \cdots, \ r_3 \not\equiv 0 \ (\mathfrak{q}_3)$. Aber nach Bedingung (I) muss eine solche Kette im Endlichen abbrechen und schliesslich muss das zu $\mathfrak{q}_n = (a):(r_n) = (a):(r_n^2) = \cdots$ gehörige Halbprimideal $\mathfrak{h}_n$ für eine grosse Zahl n prim und ferner $r_n \not\equiv 0 \ (\mathfrak{q}_n)$ sein.

(1) Mit Hilfe des Wohlordnungssatzes hat W. Krull schon die Existenz eines minimalen Primoberideals eines Hauptideals im allgemeinen Ring veröffentlicht: Math. Annalen **101** (1929), Idealtheorie in Ringen ohne Endlichkeitsbedingung. Hier benutzen wir aber nur unsere Bedingung I.

Setzen wir nun $\mathfrak{h}_n=\mathfrak{p}$ und ist $\mathfrak{p}'\subset\mathfrak{p}$ für ein Primideal-teiler $\mathfrak{p}'$ von (a), so wird $r_n\not\equiv 0\ (\mathfrak{p})$ und es gibt ein Element p von der Art, dass $p\equiv 0\ (\mathfrak{p})$, $p\not\equiv 0\ (\mathfrak{p}')$ ist, und für eine grosse Zahl m gilt $p^m r_n\equiv 0\ (a)$. Da aber $p^m\not\equiv 0\ (\mathfrak{p}')$ ist, so muss damit $r_n\equiv 0\ (\mathfrak{p}')$ entgegen $r_n\not\equiv 0\ (\mathfrak{p})$ sein. Also muss $\mathfrak{h}_n=\mathfrak{p}$ ein höchstes Primideal von (a) sein.

Für die Anzahl der höchsten Primideale eines Hauptideals in $\mathfrak{J}$ gilt ferner der

Satz 12. *Gilt in $\mathfrak{J}$ Bedingung I, so ist die Anzahl der höchsten Primideale eines Hauptideals (a) in $\mathfrak{J}$ endlich, und der Durchschnitt aller höchsten Primideale von (a) ist mit dem zu (a) gehörigen Halbprimideal identisch.*

Zum Beweise dürhen wir annehmen, dass (a) kein Primideal ist. Nach Satz 11 existiert ein höchstes Primideal $\mathfrak{p}$ von (a). Ist ein durch $\mathfrak{p}$ unteilbares Element r' ein Nullteiler in bezug auf (a), so wird $(a)\subset\mathfrak{r}'=(a):(r')$. Aber wegen Bedingung I muss endlich jedes durch $\mathfrak{p}$ unteilbare Element kein Nullteiler in bezug auf $\mathfrak{r}^{(k)}=(a):(r'r''\ldots.r^{(k)})$ sein. Wenn $\mathfrak{r}^{(k)}$ nicht prim ist, so wird auch $\mathfrak{r}^{(k)}\subset(a):(r'\ldots.r^{(k)}\bar{r}')$ für ein durch $\mathfrak{r}^{(k)}$ unteilbares Element $\bar{r}'$ aus $\mathfrak{p}$. Da $\mathfrak{p}$ ein höchstes Primideal von (a) ist, so erhalten wir damit nach Bedingung I $\mathfrak{p}=(a):(b)$ für ein Element b.

Es seien nun $\mathfrak{p}_1,\mathfrak{p}_2,\ldots.$ alle höchsten Primideale von (a), dann nach dem soeben gewonnenen Ergebnis

$$(1)\qquad \mathfrak{p}_1=(a):(b_1),\quad \mathfrak{p}_2=(a):(b_2),\ldots.$$

Setzen wir nun

$$(2)\quad \mathfrak{d}_1=\mathfrak{p}_1,\quad \mathfrak{d}_2=[\mathfrak{p}_1,\mathfrak{p}_2],\ldots.,\quad \mathfrak{q}_1=(a):\mathfrak{d}_1,\quad \mathfrak{q}_2=(a):\mathfrak{d}_2,\ldots.,$$

dann wird $\mathfrak{q}_1\subset\mathfrak{q}_2\subset\mathfrak{q}_3\subset\cdots.$ Denn nach (1) und (2) erhalten wir $(b_1,b_2,\ldots.b_i)\equiv 0\ (\mathfrak{q}_i)$, $(b_1,\ldots.,b_i,b_{i+1})\equiv 0\ (\mathfrak{q}_{i+1})$ und $\mathfrak{q}_i\subseteqq\mathfrak{q}_{i+1}$. Wäre $b_{i+1}\equiv 0\ (\mathfrak{q}_i)$, so würde $(b_{i+1})\,\mathfrak{p}_i\ldots.\mathfrak{p}_i\equiv 0\ (a)$ und nach (1) hätten wir einen Widerspruch $\mathfrak{p}_1\ldots.\mathfrak{p}_i\equiv 0\ (\mathfrak{p}_{i+1})$. Also muss $b_{i+1}\not\equiv 0\ (\mathfrak{q}_i)$ und folglich $\mathfrak{q}_i\subset\mathfrak{q}_{i+1}$ sein. Wegen Bedingung I muss damit die Anzal der verschiedenen höchsten Primideale von (a) endlich sein.

Es sei $\mathfrak{d}$ der Durchschnitt aller höchsten Primideale von (a), dann ist $\mathfrak{d}$ ein Teiler des zu (a) gehörigen Halbprimideals $\mathfrak{h}$. Ist ein Element d aus $\mathfrak{d}$ durch $\mathfrak{h}$ unteilbar, so ist nach dem Beweise von Satz 11

$$\mathfrak{q}_n=(a):(r_n)=(a):(r_n^2)=\cdots.,\quad r_n\not\equiv 0\ (\mathfrak{q}_n),\ r_n\equiv 0\ (d).$$

Dabei ist das zu $\mathfrak{q}_n$ gehörige Halbprimideal $\mathfrak{p}$ ein höchstes Primideal von (a) und ferner muss $r_n \not\equiv 0\ (\mathfrak{p})$ sein. Anderseits ist aber r_n durch alle höchsten Primideale von (a) teilbar und damit ergibt sich ein Widerspruch. Also muss $\mathfrak{d}=\mathfrak{h}$ sein.

Für die spätere Benutzung fügen wir noch einen Satz hinzu.

Satz 13. *Es sei $\mathfrak{J}$ ein Integritätsbereich mit Bedingung I und $\mathfrak{p}$ ein höchstes Primideal eines Hauptideals (a). Dann muss der Durchschnitt $\mathfrak{d}$ aller $(a):(r_1)$, $(a^2):(r_2)$, $(a^3):(r_3),\ldots$. Nullideal sein, wenn $r_1, r_2, r_3, \ldots$ eine beliebige Reihe der durch $\mathfrak{p}$ unteilbaren Elemente ist.*

Zum Beweise sei es d ein von Null verschiedenes Element aus $\mathfrak{d}$. Dann wird

$$(1) \qquad dr_1=ab_1,\quad dr_2=a^2b_2,\ldots,\quad dr_i=a^ib_i,\ldots.$$

Betrachten wir die Idealquotienten-kette $(d):(a)\subseteqq(d):(a^2)\subseteqq\cdots\subseteqq\cdots$ $(d):(a^i)\subseteqq\cdots$, so erhalten wir nach Bedingung I $(d):(a^n)=(d):(a^{n+1})$ für eine ganze Zahl n und daraus folgt nach (1)

$$dr_{n+1}=a^{n+1}b_{n+1} \qquad dr=a^nb_{n+1}.$$

Daher ergibt sich $r_{n+1}=ra\equiv 0\ (\mathfrak{p})$. Das widerspricht unserer Voraussetzung $r_{n+1}\not\equiv 0\ (\mathfrak{p})$. Damit muss $d=0$ sein, also ist unsere Behauptung bewiesen.

Um die bis jetzt entwickelte Theorie in $\mathfrak{J}$ bis zu der gewünschten zu entwickeln, nehmen wir zu Bedingung I noch die folgende hinzu:

Bedingung II. *Jedes höchste Primideal eines beliebigen Hauptideals aus $\mathfrak{J}$ ist stets umkehrbar.*

Dann gilt zunächst der

Satz 14. *Sind in $\mathfrak{J}$ Bedingungen I und II beide erfüllt, so ist jedes höchste Primideal eines beliebigen Hauptideals ein in $\mathfrak{J}$ minimales Primideal.*

Es sei (a) ein beliebiges Hauptideal in $\mathfrak{J}$ und $\mathfrak{p}$ ein höchstes Primideal von (a). Dann ist nach Bedingung II $\mathfrak{p}\mathfrak{p}^{-1}=\mathfrak{J}$. Ist ein Primideal $\mathfrak{p}'$ durch $\mathfrak{p}$ teilbar, so muss $(a)\not\equiv 0\ (\mathfrak{p}')$ sein, weil $\mathfrak{p}$ ein höchstes Primideal von (a) ist. Nehmen wir ein Element p' von $\mathfrak{p}'$ aus, so muss nach Satz 12 ein höchstes Primideal $\mathfrak{p}''$ von (p') durch $\mathfrak{p}'$ teilbar sein. Aus $\mathfrak{p}\mathfrak{p}^{-1}=\mathfrak{J}$ folgt damit $\mathfrak{p}''\mathfrak{p}^{-1}=\mathfrak{a}$, wo $\mathfrak{a}$ ein Ideal in $\mathfrak{J}$ bedeutet, und daraus ergibt sich $\mathfrak{p}''=\mathfrak{a}\mathfrak{p}$, $\mathfrak{a}\equiv 0\ (\mathfrak{p}'')$. Also ist $\mathfrak{p}''=\mathfrak{p}''\mathfrak{p}$. Andererseits ist aber nach Bedingung II auch $\mathfrak{p}''\mathfrak{p}''^{-1}=\mathfrak{J}$ und folglich erhalten wir danach einen Widerspruch $\mathfrak{p}=\mathfrak{J}$. Damit muss $\mathfrak{p}$ ein in $\mathfrak{J}$ minimales Primideal sein.

Über die Eigenschaften eines umkehrbaren, minimalen Primideals beweisen wir den

Satz 15. *Es gelte in* $\mathfrak{J}$ *Bedingung I und es sei* $\mathfrak{p}$ *ein in* $\mathfrak{J}$ *minimales Primideal und umkehrbar. Dann ist*

I $\mathfrak{p}^n \neq \mathfrak{p}^{n+1}$ *für jede ganze Zahl* n,

II $\mathfrak{p}^n$ *stets primär,*

III $p \equiv 0\ (\mathfrak{p}^k),\ \not\equiv 0\ (\mathfrak{p}^{k+1})$ *für eine endliche ganze Zahl* k,

wenn p *ein beliebiges, von Null verschiedenes Element aus* $\mathfrak{p}$ *ist.*

Nehmen wir $\mathfrak{p}^n = \mathfrak{p}^{n+1}$ an, so folgt aus $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{J}$ ein Widerspruch $\mathfrak{p} = \mathfrak{J}$. Also muss $\mathfrak{p}^n \neq \mathfrak{p}^{n+1}$ für jede ganze Zahl n sein.

Es sei p ein solches Element, dass $p \equiv 0\ (\mathfrak{p})$, $\not\equiv 0\ (\mathfrak{p}^n)$ ist. Dann wird $p \equiv 0\ (\mathfrak{p}^s)$, $\not\equiv 0\ (\mathfrak{p}^{s+1})$ für eine ganze Zahl $s\ (0 < s < n)$. Aus $\mathfrak{p}^s\mathfrak{p}^{-s} = \mathfrak{J}$ folgt damit

$$(1) \qquad (p) = \mathfrak{a}\mathfrak{p}^s, \quad \mathfrak{a} \not\equiv 0\ (\mathfrak{p}),$$

dabei ist $\mathfrak{a}$ ein Ideal in $\mathfrak{J}$. Wäre für ein durch $\mathfrak{p}$ unteilbares Element r $rp \equiv 0\ (\mathfrak{p}^n)$, so folgte aus $\mathfrak{p}^n\mathfrak{p}^{-n} = \mathfrak{J}$ auch

$$(2) \qquad (rp) = \mathfrak{a}'\mathfrak{p}^n,$$

wo $\mathfrak{a}'$ ein Ideal aus $\mathfrak{J}$ bedeutet. Aus (1) und (2) hätten wir $(r)\mathfrak{a}\mathfrak{p}^s = \mathfrak{a}'\mathfrak{p}^n$, und daher folgte $(r)\mathfrak{a} = \mathfrak{a}'\mathfrak{p}^{n-s}$ $(0 < n-s < n)$, $\mathfrak{a} \not\equiv 0\ (\mathfrak{p})$, $(r) \not\equiv 0\ (\mathfrak{p})$. Das widerspricht der Eigenschaft vom Primideal $\mathfrak{p}$, also muss $\mathfrak{p}^n$ stets primär sein.

Nach dem ersten Fall ist $\mathfrak{p}^i \neq \mathfrak{p}^{i+1}$ und wir können ein durch $\mathfrak{p}^2$ unteilbares Element p_1 aus $\mathfrak{p}$ finden. Aus $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{J}$ folgt $p_1 = \mathfrak{p}\mathfrak{a}_1$, $\mathfrak{a}_1 \not\equiv 0\ (\mathfrak{p})$ und damit muss nach I und II $p_1^i \equiv 0\ (\mathfrak{p}^i)$, $\not\equiv 0\ (\mathfrak{p}^{i+1})$ sein. Daher folgt auch aus $\mathfrak{p}^i\mathfrak{p}^{-i} = \mathfrak{J}$ $(p_1^i) = \mathfrak{p}^i\mathfrak{a}_i$, $\mathfrak{a}_i \not\equiv 0\ (\mathfrak{p})$. Da $\mathfrak{p}^i$ aber nach dem zweiten Fall primär ist, so wird $\mathfrak{p}^i = (p_1^i) : (a_i)$ für ein durch $\mathfrak{p}$ unteilbares Element a_i. Nach Satz 13 ist damit der Durchschnitt aller $\mathfrak{p}^i$ Nullideal und folglich gibt es eine solche Zahl k, dass $p \equiv 0\ (\mathfrak{p}^k)$, $\not\equiv 0\ (\mathfrak{p}^{k+1})$ ist.

Setzen wir statt Bedingung II die Folgende Bedingung voraus:

Bedingung II′. *Jedes Primideal aus* $\mathfrak{J}$ *enthält irgendein in* $\mathfrak{J}$ *minimales Primideal, und jedes in* $\mathfrak{J}$ *minimale Primideal ist umkehrbar,*

so ergibt sich zunächst

Satz 16. *Wenn in* $\mathfrak{J}$ *Bedingungen I und II′ beide gelten, so sind alle zu einem beliebigen Hauptideal gehörigen Primideale*(1) *stets ein in* $\mathfrak{J}$ *minimales Primideal.*

(1) Ein von $\mathfrak{J}$ verschiedenes Primideal $\mathfrak{p}$ heisst das „*zum Hauptideal* (a) *gehörige Primideal*“, wenn für ein Element r aus $\mathfrak{J}$ $\mathfrak{p} = (a) : (r)$ ist.

Es sei (a) ein beliebiges Hauptideal in $\mathfrak{J}$ und $\mathfrak{p}$ ein zu (a) gehöriges Primideal, dann erhalten wir für ein Element r

$$(1) \qquad \mathfrak{p}=(a):(r), \quad r \not\equiv 0 \ (a), \quad \mathfrak{p}(r)\equiv 0 \ (a).$$

Nach Bedingung II′ muss ein in $\mathfrak{J}$ minimales Primideal $\mathfrak{p}'$ durch $\mathfrak{p}$ teilbar sein. Zum Beweise setzen wir nun $\mathfrak{p}\supset\mathfrak{p}'$ voraus, und wir unterscheiden zwei verschiedene Fälle, je nachdem a zu $\mathfrak{p}'$ gehört, oder nicht.

1. Es sei $a \not\equiv 0 \ (\mathfrak{p}')$. Dann aus (1) folgt $\mathfrak{p}'(r)=(a)\mathfrak{a}'$ für ein Ideal $\mathfrak{a}'$ und $\mathfrak{a}'\equiv 0 \ (\mathfrak{p}')$. Aber nach Bedingung II′ ist $\mathfrak{p}'\mathfrak{p}'^{-1}=\mathfrak{J}$, und daraus erhalten wir $(r)=(a)\mathfrak{a}'\mathfrak{p}'^{-1}$. Dabei ist aber $\mathfrak{a}'\mathfrak{p}'^{-1}$ ein Ideal in $\mathfrak{J}$ und danach ergibt sich ein Widerspruch $r\equiv 0 \ (a)$ zu (1).

2. Es sei $a\equiv 0 \ (\mathfrak{p}')$. Dann gilt nach Satz 15 $(a)\equiv 0 \ (\mathfrak{p}'^k)$, $\not\equiv 0 \ (\mathfrak{p}'^{k+1})$ für eine von Null verschiedene ganze Zahl k. Da $\mathfrak{p}'^k$ auch nach Satz 15 primär ist, so folgt aus (1) $r=0 \ (\mathfrak{p}'^k)$. Aus (1) und $\mathfrak{p}\supset\mathfrak{p}'$ folgt $\mathfrak{p}'(r)=\mathfrak{a}''(a)$ für ein Ideal $\mathfrak{a}''$ aus $\mathfrak{J}$, und dabei muss $\mathfrak{a}''\equiv 0 \ (\mathfrak{p}')$ sein, weil $(a) \not\equiv 0 \ (\mathfrak{p}'^{k+1})$; $r\equiv 0 \ (\mathfrak{p}'^k)$ und $\mathfrak{p}'^{k+1}$ primär ist. Damit muss $\mathfrak{a}''\mathfrak{p}'^{-1}=\mathfrak{a}'''$ ein Ideal in $\mathfrak{J}$ sein. Durch Multiplikation mit $\mathfrak{p}'^{-1}$ erhalten wir danach

$$\mathfrak{p}'\mathfrak{p}'^{-1}(r)=\mathfrak{a}''\mathfrak{p}'^{-1}(a), \quad (r)=\mathfrak{a}'''(a), \quad r\equiv 0 \ (a).$$

Das widerspricht unserer Voraussetzung (1).

Hiermit muss $\mathfrak{p}=\mathfrak{p}'$ sein und unser Satz ist bewiesen.

Wir können nun die Äquivalenz der beiden Bedingungen II und II′ beweisen.

Satz 17. *Ist in $\mathfrak{J}$ die Bedingung I erfüllt, so sind die beiden Bedingungen II und II′ in $\mathfrak{J}$ äquivalent.*

Gilt in $\mathfrak{J}$ Bedingung II, so ist nach Satz 14 jedes höchste Primideal eines Hauptideals ein in $\mathfrak{J}$ minimales Primideal. Da nach Satz 12 die Anzahl der höchsten Primideale endlich ist, so enthält ein beliebiges Primideal aus $\mathfrak{J}$ somit ein in $\mathfrak{J}$ minimales Primideal. Ferner folgt es aus Bedingung II, dass jedes in $\mathfrak{J}$ minimale Primideal umkehrbar sein muss.

Wir nehmen in $\mathfrak{J}$ die Gültigkeit der Bedingung II′ an. Nach Satz 11 besitzt ein beliebiges Hauptideal (a) aus $\mathfrak{J}$ sein höchstes Primideal $\mathfrak{p}$ und nach dem Beweise von Satz 12 gilt $\mathfrak{p}=(a):(b)$ für ein Element b. Also ist $\mathfrak{p}$ ein zu (a) gehöriges Primideal und nach Satz 16 muss $\mathfrak{p}$ ein in $\mathfrak{J}$ minimales Primideal sein. Wegen Bedingung II′ ist damit jedes höchste Primideal eines Hauptideals immer umkehrbar.

Der Hauptsatz und seine Folgerungen.

Als das Hauptziel dieser Arbeit beweisen wir jetzt mit Hilfe der in den vorigen Paragraphen entwickelten Ergebnisse den

Hauptsatz I. *Die notwendige und hinreichende Bedingung dafür, dass ein beliebiges Hauptideal eines Integritätsbereiches $\mathfrak{J}$ mit Einselement sich als Potenzprodukt von endlich vielen Primidealen darstellen lässt, besteht darin, dass in $\mathfrak{J}$ die folgenden Bedingungen erfüllt sind:*

I. *Ist (a) ein beliebiges Hauptideal in $\mathfrak{J}$, so bricht die Idealquotienten-kette $(a):\mathfrak{a}_1 \subset (a):\mathfrak{a}_2 \subset (a):\mathfrak{a}_3 \subset \cdots$ nach endlich vielen Gliedern ab.*

II. *Jedes höchste Primideal eines beliebigen Hauptideals aus $\mathfrak{J}$ ist stets umkehrbar.*

Aus Sätzen 8, 9 und 10 ergibt sich unmittelbar, dass diese Bedingungen notwendig sind. Um die Hinreichbarkeit der Bedingungen zu beweisen, sei (a) ein beliebiges Hauptideal in $\mathfrak{J}$. Dann besitzt (a) nach Sätze 11 und 12 seine endlich viele minimale Primoberideale $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ und $\mathfrak{p}_i$ sind nach Satz 14 ein in $\mathfrak{J}$ minimales Primideal und ferner geben nach Satz 15 die ganzen Zahlen k_i von der Art, dass

$$(1) \qquad (a) \equiv 0 \ (\mathfrak{p}_i^{k_i}), \ \not\equiv 0 \ (\mathfrak{p}_i^{k_i+1}) \quad (i=1, 2, \ldots, n)$$

ist. Da nach Bedingung II $\mathfrak{p}_i^{k_i}\mathfrak{p}_i^{-k_i}=\mathfrak{J}$ ist, so erhalten wir aus (1)

$$(2) \qquad (a)=\mathfrak{p}_i^{k_i}\mathfrak{a}_i, \quad \mathfrak{a}_i \not\equiv 0 \ (\mathfrak{p}_i) \quad (i=1, 2, \ldots, n),$$

wobei $\mathfrak{a}_i$ ein Ideal in $\mathfrak{J}$ ist. Andererseits is nach Satz 15 $\mathfrak{p}_i^{k_i}$ primär und $\mathfrak{p}_i^{k_i} \neq \mathfrak{p}_i^{k_i+1}$ und daher erhalten wir aus (2)

$$(3) \qquad (a)=\mathfrak{p}_1^{k_1}\mathfrak{p}_2^{k_2}\ldots\mathfrak{p}_n^{k_n}\mathfrak{a}, \quad \mathfrak{a} \not\equiv 0 \ (\mathfrak{p}_i) \quad (i=1, 2, \ldots, n).$$

Denn aus $(a)=\mathfrak{p}_1^{k_1}\mathfrak{a}_1=\mathfrak{p}_2^{k_2}\mathfrak{a}_2$ folgt $\mathfrak{a}_2 \equiv 0 \ (\mathfrak{p}_1^{k_1})$ und nach $\mathfrak{p}_1^{k_1}\mathfrak{p}_1^{-k_1}=\mathfrak{J}$ haben wir daraus $\mathfrak{a}_2=\mathfrak{a}_2'\mathfrak{p}_1^{k_1}$, oder $(a)=\mathfrak{p}_1^{k_1}\mathfrak{p}_2^{k_2}\mathfrak{a}_2'$. Nach $(n-1)$-maliger Wiederholung dieses Verfahrens erhalten wir endlich Beziehung (3). Ist $(a)=\mathfrak{p}_1^{k_1}\ldots\mathfrak{p}_n^{k_n}$, so kommt unser Beweis zum Schlusse. Damit nehmen wir $(a) \neq \mathfrak{p}_1^{k_1}\ldots\mathfrak{p}_n^{k_n}$ an. Dann können wir nach (3) ein durch (a) unteilbares Element p_0 aus $\mathfrak{p}_1^{k_1}\ldots\mathfrak{p}_n^{k_n}$ auswählen. Der Idealquotient $\mathfrak{r}_0=(a):(p_0)$ ist von $\mathfrak{J}$ verschieden, und nach (3) ist $\mathfrak{r}_0$ ein Teiler von $\mathfrak{a}$. Ist $\mathfrak{r}_0$ nicht prim, so wird $p_1p_1'\equiv 0 \ (\mathfrak{r}_0)$, $p_1 \not\equiv 0$, $p_1' \not\equiv 0 \ (\mathfrak{r}_0)$ und $\mathfrak{r}_0 \subset \mathfrak{r}_1=(a):(p_0p_1) \neq \mathfrak{J}$. Nach Bedingung I erhalten wir auf solcher Weise end-

lich ein Primideal $\mathfrak{p}=(a):(p)\neq\mathfrak{J}$. Da $\mathfrak{p}$ danach ein zu (a) gehöriges Primideal ist, so muss $\mathfrak{p}$ nach Sätze 16 und 17 ein in $\mathfrak{J}$ minimales Primideal und folglich mit einem, etwa $\mathfrak{p}_1$, aus $\mathfrak{p}_i$ $(i=1, 2, \ldots, n)$ identisch sein. Anderseits ist aber $\mathfrak{a}\equiv 0\ (\mathfrak{p})$, oder $\mathfrak{a}\equiv 0\ (\mathfrak{p}_1)$ und wir haben einen Widerspruch zu (3). Damit muss $(a)=\mathfrak{p}_1^{k_1}\mathfrak{p}_2^{k_2}\ldots\mathfrak{p}_n^{k_n}$ sein, und unser Hauptsatz ist in alle seinen Tellen vollständig bewiesen.

Nach Satz 17 lässt sich der Hauptsatz auch in der folgenden Form besprechen:

Hauptsatz II. *Damit in einem Integritätsbereich $\mathfrak{J}$ mit Einselement jedes Hauptideal als Potenzprodukt von endlich vielen Primidealen darstellbar ist, ist notwendig und hinreichend, dass*

I *jede Idealquotienten-kette*

$$(a):\mathfrak{a}_1\subset(a);\ \mathfrak{a}_2\subset(a):\mathfrak{a}_3\subset\cdots$$

im Endlichen abbricht,

II *jedes Primideal aus $\mathfrak{J}$ irgend ein in $\mathfrak{J}$ minimales Primideal enthält und jedes in $\mathfrak{J}$ minimale Primideal umkehrbar ist.*

Als ein spezieller Fall ergibt sich aus dem letzten Hauptsatze der wichtige

Satz. *Ist $\mathfrak{J}$ ein Integritätsbereich mit dem Teilerkettensatz, so lässt sich jedes Hauptideal in $\mathfrak{J}$ dann und nur dann als Potenzprodukt von endlich vielen Primidealen darstellen, wenn jedes in $\mathfrak{J}$ minimale Primideal umkehrbar ist.*

Denn in $\mathfrak{J}$ ist Bedingung I in Hauptsatz II offenbar erfüllt, und nach dem Hauptidealsatz[1] muss jedes Primideal aus $\mathfrak{J}$ irgend ein in $\mathfrak{J}$ minimales Primideal stets enthalten. Damit folgt unser Satz unmittelbar aus Hauptsatz II.

Als eine andere Folgerung von Hauptsatz II bekommen wir auch den

Satz. *Notwendig und hinreichend dafür, dass jedes Ideal vom Integritätsbereich $\mathfrak{J}$ mit Einselement sich als Potenzprodukt von endlich vielen Primidealen darstellen lässt, ist, dass*

1 *in $\mathfrak{J}$ der Teilerkettensatz gilt,*

2 *jedes Primideal in $\mathfrak{J}$ umkehrbar ist.*

Ist jedes Ideal aus $\mathfrak{J}$ als Potenzprodukt von endlich vielen Primidealen darstellbar, so existiert nach Hauptsatz II ein in $\mathfrak{J}$ minimales

(1) W. Krull, *Idealtheorie*, 37.

Primideal $\mathfrak{p}$ und $\mathfrak{p}$ ist umkehrbar. Ist r ein durch $\mathfrak{p}$ unteilbares Element aus $\mathfrak{J}$ und $(r, \mathfrak{p}) \neq \mathfrak{J}$, so wird

$$(1) \quad (r, \mathfrak{p}) = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_m, \quad (r^2, \mathfrak{p}) = \mathfrak{p}_1' \mathfrak{p}_2' \dots \mathfrak{p}_n', \quad (r, \mathfrak{p}) \neq (r^2, \mathfrak{p}),$$

wo jedes $\mathfrak{p}_i, \mathfrak{p}_j'$ ein Primidealteiler von $\mathfrak{p}$ bedeutet. Im Restklassenring $\bar{\mathfrak{J}} = \mathfrak{J}/\mathfrak{p}$ ergibt sich nach (1)

$$(2) \qquad (r) = \bar{\mathfrak{p}}_1 \bar{\mathfrak{p}}_2 \dots \bar{\mathfrak{p}}_m, \quad (r^2) = \bar{\mathfrak{p}}_1' \bar{\mathfrak{p}}_2' \dots \bar{\mathfrak{p}}_n',$$

wo $\bar{\mathfrak{p}}_i$ ein Primideal aus $\bar{\mathfrak{J}}$ bedeutet, welches dem Primideal $\mathfrak{p}_i$ entspricht. Da $\bar{\mathfrak{J}}$ ein Integritätsbereich mit Einselement ist, und da jedes Hauptideal in $\bar{\mathfrak{J}}$ als Potenzprodukt von endlich vielen Primidealen aus $\bar{\mathfrak{J}}$ darstellbar ist, so muss nach (2) $\bar{\mathfrak{p}}_1^2 \bar{\mathfrak{p}}_2^2 \dots \bar{\mathfrak{p}}_m^2 = \bar{\mathfrak{p}}_1' \bar{\mathfrak{p}}_2' \dots \bar{\mathfrak{p}}_n'$ und $\bar{\mathfrak{p}}_1^2$ primär sein. Daher erhalten wir in $\mathfrak{J}$ $(r, \mathfrak{p})^2 = (r^2, \mathfrak{p})$ oder $\mathfrak{p}(r, \mathfrak{p}) = \mathfrak{p}$. Da nach Hauptsatz II $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{J}$ ist, ergibt sich ein Widerspruch $(r, \mathfrak{p}) = \mathfrak{J}$ gegen unsere Voraussetzung. Folglich muss $\mathfrak{p}$ ein maximales Ideal in $\mathfrak{J}$ sein, und daher folgt die Notwendigkeit von Bedingung II. In der Produktdarstellung eines Ideals $\mathfrak{a}$ ist jedes Primideal nach dem soeben gewonnenen Ergebnis ein in $\mathfrak{J}$ minimales Primideal und seine Potenz ist stets primär. Daraus folgt leicht die Notwendigkeit der Bedingung I.

Wir setzen in $\mathfrak{J}$ die Gültigkeit der Bedingungen 1 und 2 voraus. Dann gibt es ein von Null verschiedenes Primideal $\mathfrak{p}$ in $\mathfrak{J}$. Ist $\mathfrak{p}$ durch ein anderes Ideal $\mathfrak{a}$ teilbar, so ist $\mathfrak{a}$ nach Bedingung 1 durch ein von $\mathfrak{J}$ verschiedenes Primideal $\mathfrak{p}'$ teilbar und daraus folgt nach Bedingung 2 $\mathfrak{p} = \mathfrak{a}_1 \mathfrak{p}'$ für ein Ideal $\mathfrak{a}_1$ aus $\mathfrak{J}$, da $\mathfrak{p}'\mathfrak{p}'^{-1} = \mathfrak{J}$ ist. Daraus folgt $\mathfrak{a}_1 \equiv 0\ (\mathfrak{p})$ und $\mathfrak{p} = \mathfrak{p}\mathfrak{p}'$. Nach $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{J}$ erhalten wir damit einen Widerspruch $\mathfrak{p}' = \mathfrak{J}$. Also muss ein Primideal $\mathfrak{p}$ in $\mathfrak{J}$ stets ein maximales Ideal sein. Nach Hauptsatz II gilt aber $(a) \equiv \mathfrak{p}_1^{k_1} \mathfrak{p}_2^{k_2} \dots \mathfrak{p}_n^{k_n}$ für ein beliebiges Element a eines Ideals $\mathfrak{a}$. Wäre $\mathfrak{a}$ durch jedes Primideal $\mathfrak{p}_i$ unteilbar, so müsste $(\mathfrak{p}_i, \mathfrak{a}) = \mathfrak{J}$ $(i = 1, 2, \dots, n)$ und folglich $\big((a), \mathfrak{a}\big) = \mathfrak{J}$ sein, da $\mathfrak{p}_i$ ein maximales Ideal ist. Folglich muss $\mathfrak{a}$ durch eines, etwa $\mathfrak{p}_1$, aus $\mathfrak{p}_i$ $(i = 1, 2, \dots, n)$ teilbar und $\mathfrak{a} = \mathfrak{p}_1 \mathfrak{a}'$ sein. Auf gleicher Weise erhalten wir wieder $\mathfrak{a}' = \mathfrak{p}_2 \mathfrak{a}''$, $\mathfrak{a} = \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{a}''$. Da $(a) \equiv 0\ (\mathfrak{a})$ ist, so muss dieses Verfahren nach einer endlichen Anzahl von Schritten ein Ende nehmen, und wir erhalten schliesslich $\mathfrak{a} = \mathfrak{p}_1^{a_1} \mathfrak{p}_2^{a_2} \dots \mathfrak{p}_m^{a_m}$.