

Ueber Produktzerlegung der Ideale.

Shinziro MORI.

(Eingegangen am 9, 11, 1931.)

Bekanntlich ist es nicht allgemein möglich, jedes Ideal als Produkt von Primäridealien darzustellen. Es fragt sich demnach, in welchem Ring jedes Ideal sich stets als Produkt von Primäridealien darstellen lässt. Wir haben noch keine allgemeine Antwort auf diese Frage; in der vorliegenden Note wird aber eine Charakterisierung aller derjenigen Ringe gegeben, in denen das Produkt aller Primärkomponenten in jeder kürzesten Durchschnittsdarstellung eines Ideals stets gleich dem Ideal ist.

Zugrunde gelegt sei ein kommutativer Ring $\mathfrak{R}$ mit Teilerkettensatz, und sei das Zeichen $\alpha = [q_1, \dots, q_n]$ immer eine kürzeste Darstellung von α durch grösste Primäridealien. Ein vom Einheitsideal $\mathfrak{o}$ verschiedenes Ideal, das keinen echten Teiler ausser $\mathfrak{o}$ besitzt, heisst ein „*maximales Ideal*,“ und unter dem „*maximalen Primideal*“ verstehen wir ein von $\mathfrak{o}$ verschiedenes Primideal, das kein von $\mathfrak{o}$ verschiedenes Primideal als echten Teiler besitzt.

§ 1. Zur Gleichung $\alpha\mathfrak{b} = \alpha$.

Als eine Verallgemeinerung eines Satzes⁽¹⁾ für den idempotenten Ring gilt der folgende

Satz 1. *Ist α ein beliebiges Ideal, und ist $\mathfrak{b}$ auch ein Ideal, so wird dann und nur dann*

$$\alpha\mathfrak{b} = \alpha,$$

wenn es in $\mathfrak{b}$ ein Element b gibt, derart, dass für jedes Element a aus α

$$ab = a$$

ist.

(1) S. Mori, Ueber Ringe, in denen die grössten Primärkomponenten jedes Ideals eindeutig bestimmt sind, dieses Journal, 1 (1931), § 4.

Zum Beweis nehmen wir zunächst an, dass

$$ab = a \neq (0).$$

Dann wird offenbar

$$(1) \quad a = ab = ab^2 = \dots \neq (0),$$

folglich soll b kein nilpotentes Ideal sein. Setzen wir jetzt

$$a = (a_1, a_2, \dots, a_m), \quad b = (b_1, b_2, \dots, b_n),$$

so ist damit wenigstens eines aus b_i nicht nilpotent. Wenn $b_1, b_2, \dots, b_k$ diejenigen aus b_i sind, die nicht nilpotent sind, so folgt aus (1)

$$a = a \cdot (b_1^\rho, b_2^\rho, \dots, b_k^\rho) = a \cdot (b_1^{m\rho}, b_2^{m\rho}, \dots, b_k^{m\rho})$$

für eine passend grosse Zahl ρ , folglich wird

$$(2) \quad \begin{aligned} a &= (a_1 b_1^\rho, \dots, a_i b_j^\rho, \dots, a_m b_k^\rho) \\ &= (a_1 b_1^{m\rho}, \dots, a_i b_j^{m\rho}, \dots, a_m b_k^{m\rho}). \end{aligned}$$

Dabei muss wenigstens eines aus $a_i b_j^{m\rho}$ von Null verschieden sein, da $a \neq (0)$ ist. Es sei damit

$$(3) \quad a_s b_t^{m\rho} \neq 0.$$

Aus (2) folgen

$$\begin{aligned} a_1 &= b_{11}a_1 + b_{12}a_2 + \dots + b_{1m}a_m, \\ a_2 &= b_{21}a_1 + b_{22}a_2 + \dots + b_{2m}a_m, \\ &\dots\dots\dots \\ &\dots\dots\dots \\ a_m &= b_{m1}a_1 + \dots\dots\dots + b_{mm}a_m, \end{aligned}$$

wo b_{ij} die Elemente aus b sind. Durch Multiplikation mit b_t^ρ folgen

$$\begin{aligned} a_1(b_{11}b_t^\rho - b_t^\rho) + \dots\dots\dots + a_m b_{1m}b_t^\rho &= 0, \\ a_1 b_{21}b_t^\rho + a_2(b_{22}b_t^\rho - b_t^\rho) + \dots + a_m b_{2m}b_t^\rho &= 0, \\ &\dots\dots\dots \\ &\dots\dots\dots \\ a_1 b_{m1}b_t^\rho + \dots\dots\dots + a_m(b_{mm}b_t^\rho - b_t^\rho) &= 0. \end{aligned}$$

Durch Elimination erhalten wir die Beziehung

$$a_s \begin{vmatrix} b_{11}b_t^p - b_t^p, & b_{12}b_t^p, & \dots, & b_{1m}b_t^p \\ b_{21}b_t^p, & b_{22}b_t^p - b_t^p, & \dots & \\ & \dots\dots\dots & & \\ & \dots\dots\dots & & \\ b_{m1}b_t^p, & \dots\dots\dots, & b_{mm}b_t^p - b_t^p & \end{vmatrix} = 0.$$

Hieraus folgt wegen (3)

$$a_s b_t^{mp} = b a_s b_t^{mp} \neq 0, \quad b \neq 0, \quad b \equiv 0 \quad (b).$$

Da b aber von der Auswahl von a_s und b_t^p unabhängig ist, so werden

$$a_i b_j^{mp} = b a_i b_j^{mp} \quad (i = 1, 2, \dots, m, j = 1, 2, \dots, k).$$

Für jedes Element a aus $\mathfrak{A}$ wird damit wegen (2) $ab = a$; womit die Bedingung notwendig ist.

Umgekehrt ist die Bedingung auch hinreichend; also ist der Satz vollständig bewiesen.

Zusatz. Wenn für jedes Element a stets $(a) = oa$ ist, so gibt es in $\mathfrak{A} (\neq (0))$ das Einheitselement.

Wir zeigen zunächst, dass in $\mathfrak{A}$ ein Element e existiert, für das $e^2 = e \neq 0$ ist. Ist a_1 ein beliebiges von Null verschiedenes Element, so existiert nach Satz 1 ein Element e_1 derart, dass $a_1 e_1 = a_1$ wird. Es sei α_1 die Gesamtheit aller Elemente a_1 , für die $a_1 e_1 = a_1$ ist, dann bildet α_1 ein Ideal. Ist $e_1 \equiv 0 (\alpha_1)$, so wird $e_1^2 = e_1 \neq 0$. Im anderen Falle können wir auch ein Element e_2 finden, so dass $e_1 e_2 = e_1$ wird. Die Gesamtheit α_2 aller Elemente a_2 , für die $a_2 e_2 = a_2$ ist, bildet ein Ideal, und ferner ist α_2 ein echter Teiler von α_1 . Nach dem Teilerkettensatz erhalten wir endlich ein Element e_n derart, dass $e_n^2 = e_n \neq 0$ ist.

Es sei nun $e_1'^2 = e_1' \neq 0$, und sei α_1 die Gesamtheit aller Elemente a_1 , für die $a_1 e_1' = a_1$ ist, und sei c_1 die Gesamtheit aller Elemente c_1 , für die $e_1' c_1 = 0$ ist. Dann wird unmittelbar

$$0 = c_1 + \alpha_1.$$

Ist c_1 vom Nullideal verschieden, so können wir auf gleiche Weise zeigen, dass in c_1 ein Element e_2' existiert, für das $e_2'^2 = e_2' \neq 0$ ist, und folglich wird auch für jedes Element a_2 aus α_2

$$a_2 e'_2 = a_2, \quad \mathfrak{o} = \mathfrak{c}_2 + \mathfrak{a}_2 + \mathfrak{a}_1.$$

Nach einer endlichen Anzahl von Schritten hat das Verfahren ein Ende, weil der Teilerkettensatz vorausgesetzt wird. Schliesslich erhalten wir mithin

$$\mathfrak{o} = \mathfrak{a}_1 + \mathfrak{a}_2 + \dots + \mathfrak{a}_m, \quad e'_i a_j = (0)(i \neq j), \quad e_i'^2 = e_i' \neq 0, \quad a_i e_i' = a_i$$

für jedes Element a_i aus $\mathfrak{a}_i$, und folglich wird $e = e'_1 + \dots + e'_m$ das Einheitselement von $\mathfrak{R}$.

Zusatz. Ist für beliebige Ideale $\mathfrak{a}$ und $\mathfrak{b}$ aus $\mathfrak{R}$ stets

$$[\mathfrak{a}, \mathfrak{b}] = \mathfrak{a} \cdot \mathfrak{b},$$

so wird $\mathfrak{o} = \mathfrak{a}_1 + \dots + \mathfrak{a}_m$, wo jedes $\mathfrak{a}_i$ ein Körper ist.

Falls $\mathfrak{b} = \mathfrak{o}$, so wird nach dem obigen Zusatz

$$\mathfrak{o} = \mathfrak{a}_1 + \mathfrak{a}_2 + \dots + \mathfrak{a}_m,$$

wobei $\mathfrak{a}_i$ direkt-unzerlegbar und $\mathfrak{a}_i^2 = \mathfrak{a}_i$ sind. Ferner sind $\mathfrak{a}_i$ Körper; sonst würde nach der Voraussetzung $\mathfrak{a}_i$ direkt-zerlegbar.

Durch Anwendung von Satz I ergibt sich

Satz 2. Ist $\mathfrak{a}$ ein vom Einheitsideal verschiedenes Ideal, und ist $\mathfrak{b}$ ein Teiler von $\mathfrak{a}$, so wird dann und nur dann

$$[\mathfrak{a}, \mathfrak{b}^k] = \mathfrak{a} \cdot \mathfrak{b}^k,$$

wenn es in $\mathfrak{b}^k$ ein Element b gibt, derart, dass für jedes Element d aus $\mathfrak{b} = [\mathfrak{a}, \mathfrak{b}^k]$ $bd = d$ wird.

Es seien

$$\mathfrak{a} = (a_1, a_2, \dots, a_m),$$

$$\mathfrak{b} = (\mathfrak{a}, (b_1), \dots, (b_n)) = (a_1, \dots, a_m, b_1, \dots, b_n),$$

dann wird

$$\begin{aligned} \mathfrak{b}^k &= (a_1^k, \dots, a_m^k, a_1^{k-1}b_1, \dots, b_1^k, \dots, b_n^k) \\ &= (c_1, c_2, \dots, c_l, c_{l+1}, \dots, c_{l+t}). \end{aligned}$$

Dabei ist c_i ($i = 1, 2, \dots, l$) das Produkt k Grades von beliebiger Anzahl der Elemente $a_1, \dots, a_m, b_1, \dots, b_n$, bei dem wenigstens eines aus $\mathfrak{a}_i$ stets auftritt, und c_j ($j = l+1, \dots, l+t$) ist auch das Produkt k grades von $b_1, \dots, b_n$, und dabei ist

$$l = \frac{(m+n+k-1)!}{(m+n-1)! k!} - \frac{(n+k-1)!}{(n-1)! k!}, \quad t = \frac{(n+k-1)!}{(n-1)! k!}.$$

Weiter ist offenbar

$$c_i \equiv 0 \quad (b) \quad (i = 1, 2, \dots, l).$$

Aus der Voraussetzung $[a, b^k] = ab^k$ folgen damit

$$(1) \quad c_i = a_{i1}c_1 + \dots + a_{il}c_l + a_{i,l+1}c_{l+1} + \dots + a_{i,l+t}c_{l+t},$$

wobei a_{ij} die Elemente aus a bedeuten. Ist d ein beliebiges Element aus b , so wird auch

$$(2) \quad \begin{aligned} d &= a'_1c_1 + \dots + a'_lc_l + a'_{l+1}c_{l+1} + \dots + a'_{l+t}c_{l+t} \\ &= (a'_1 + b'_1)c_1 + \dots + (a'_l + b'_l)c_l, \end{aligned}$$

wo a'_i auch die Elemente aus a , und $(a'_i + b'_i)$ die Elemente aus b sind. Die Einführung von (1) in (2) ergibt

$$d = a''_1c_1 + \dots + a''_lc_l + a''_{l+1}c_{l+1} + \dots + a''_{l+t}c_{l+t},$$

wo a''_i die Elemente aus ab sind. Ferner wird wieder

$$d = (a''_1 + b''_1)c_1 + \dots + (a''_l + b''_l)c_l,$$

wo $(a''_i + b''_i)$ die Elemente aus b^2 sind. Substituieren wir wieder hierin die Beziehungen (1), so wird auch

$$d = a'''_1c_1 + \dots + a'''_lc_l + a'''_{l+1}c_{l+1} + \dots + a'''_{l+t}c_{l+t},$$

wo a'''_i die Elemente aus ab^2 sind. Weiterführung dieses Verfahrens zeigt schliesslich, dass

$$\tilde{d} = a^{(k+1)}_1c_1 + \dots + a^{(k+1)}_lc_l + a^{(k+1)}_{l+1}c_{l+1} + \dots + a^{(k+1)}_{l+t}c_{l+t},$$

wird, wo $a^{(k+1)}_i$ die Elemente aus $b = ab^k$ sind. Daraus folgt $d \equiv 0 \pmod{ab^{2k}}$, und folglich wird

$$b = ab^k \equiv 0 \pmod{ab^{2k}}.$$

Andererseits ist offenbar $ab^{2k} \equiv 0 \pmod{ab^k}$; also wird

$$b = ab^k = (ab^k)b^k.$$

Da b^k ein Teiler von ab^k ist, so folgt wegen Satzes 1 die Existenz eines durch b^k teilbaren Elementes b von der Eigenschaft, dass für jedes Element d aus $\mathfrak{b}$ stets $db = d$ wird. Hiermit ist die Bedingung notwendig. Umgekehrt ist die Bedingung auch hinreichend, womit die Behauptung bewiesen ist.

§ 2. Sätze über die Primideale.

In diesem Paragraphen wollen wir einige wichtige Sätze für unsere spätere Untersuchung beweisen.

Satz 3. Ist $\mathfrak{p}$ ein vom Einheitsideal verschiedenes Primideal, so ist $\mathfrak{p}$ dann und nur dann teilbar durch jede Potenz von jedem echten Teiler von $\mathfrak{p}$, wenn $\mathfrak{p} = \mathfrak{p}^2$ oder $\mathfrak{p}$ ein maximales Primideal⁽¹⁾ vom Ring mit Einheitsselement ist.

Ich setze zunächst voraus, dass $\mathfrak{p}$ stets teilbar durch jede Potenz von jedem echten Teiler von sich selbst ist. Setzen wir

$$\mathfrak{p} = (p_1, p_2, \dots, p_n),$$

und ist α ein durch $\mathfrak{p}$ unteilbares Element, so wird

$$\alpha = (\mathfrak{p}, \alpha) = (p_1, \dots, p_n, \alpha)$$

ein echter Teiler von $\mathfrak{p}$. Aus der obigen Annahme folgt für jedes m

$$\mathfrak{p} \equiv 0 \ (\alpha^m).$$

Daraus folgen unmittelbar für $m \geq 2$

$$p_i = a_{i1}p_1 + \dots + a_{in}p_n + a_{in+1}\alpha \quad (i = 1, 2, \dots, n),$$

dabei sind a_{ij} die Elemente aus α . Da $\mathfrak{p}$ ein Primideal und $\alpha \not\equiv 0 \ (\mathfrak{p})$ ist, so soll

$$a_{in+1} \equiv 0 \ (\mathfrak{p}) \quad (i = 1, 2, \dots, n)$$

sein; woraus folgen

$$p_i = \alpha'_{i1}p_1 + \dots + \alpha'_{in}p_n \quad (i = 1, 2, \dots, n),$$

wo α'_{ij} auch die Elemente aus α sind. Durch Multiplikation mit α erhalten wir

(1) Wenn in $\mathfrak{A}$ das Einheitsselement existiert, so besitzt ein maximales Primideal $\mathfrak{p}$ keinen von $\mathfrak{o}$ verschiedenen echten Teiler. Vgl. den Beweis von Satz 5.

$$\begin{aligned}
 p_1(aa'_{11}-a) + \dots + p_n aa'_{1n} &= 0, \\
 p_1 aa'_{21} + p_2(aa'_{22}-a) + \dots + p_n aa'_{2n} &= 0, \\
 &\dots\dots\dots \\
 &\dots\dots\dots \\
 p_1 aa'_{n1} + \dots + p_n(aa'_{nn}-a) &= 0.
 \end{aligned}$$

Durch Elimination folgt daraus

$$p_i a^n = p_i a^n a' \quad (i = 1, 2, \dots, n),$$

wo a' ein Element aus $\mathfrak{a}$ ist. Da $\mathfrak{p}$ ein Primideal ist, so muss

$$a^n \not\equiv 0 \pmod{\mathfrak{p}}$$

sein. Wir können hier zwei verschiedene Fälle unterscheiden.

1. Fall: Es sei $a' a^n - a^n \not\equiv 0 \pmod{\mathfrak{p}}$.

Setzen wir

$$a_1 = a' a^n - a^n, \quad \mathfrak{a}_1 = (\mathfrak{p}, (a_1)),$$

so ist $\mathfrak{a}_1$ ein echter Teiler von $\mathfrak{p}$, und ferner wird

$$(1) \quad p_i a_1 = 0 \quad (i = 1, 2, \dots, n), \quad a_1^\lambda \not\equiv 0 \pmod{\mathfrak{p}} \text{ für jedes } \lambda.$$

Aus unserer Voraussetzung folgt auch für jedes λ

$$(2) \quad \mathfrak{p} \equiv 0 \pmod{\mathfrak{a}_1^\lambda}.$$

Nach (1) wird

$$\mathfrak{a}_1^\lambda = (\mathfrak{p}^\lambda, (a_1^\lambda)),$$

und ferner folgt aus (2) für $\lambda > 1$

$$p_i = p'_i + r_i a_1 \quad (i = 1, 2, \dots, n),$$

wo p'_i die Elemente aus $\mathfrak{p}^\lambda$, und r_i die Elemente aus $\mathfrak{R}$ sind. Da $a_1 \not\equiv 0 \pmod{\mathfrak{p}}$ ist, so soll $r_i \equiv 0 \pmod{\mathfrak{p}}$ sein, und folglich wird wegen (1)

$$p_i = p'_i \quad (i = 1, 2, \dots, n),$$

also wird

$$\mathfrak{p} \equiv 0 \pmod{\mathfrak{p}^\lambda}.$$

Daraus folgt

$$\mathfrak{p} = \mathfrak{p}^2.$$

2. Fall: Es sei $a'a^n - a^n \equiv 0 \pmod{\mathfrak{p}}$.

Dann werden

$$(a'^2 - a')a^n \equiv 0 \pmod{\mathfrak{p}}, \quad a' \equiv 0 \pmod{\mathfrak{a}}, \quad a' \not\equiv 0 \pmod{\mathfrak{p}},$$

da $a^n \not\equiv 0 \pmod{\mathfrak{p}}$ ist. Weiter folgt daraus

$$a'^2 - a' \equiv 0 \pmod{\mathfrak{p}}, \quad a' \not\equiv 0 \pmod{\mathfrak{p}}.$$

Setzen wir nun $\mathfrak{a}_2 = (\mathfrak{p}, (a'))$, $\mathfrak{a}'_2 = (\mathfrak{p}, (a'^2))$, so wird daher

$$(3) \quad \mathfrak{a}_2 = \mathfrak{a}'_2, \quad \mathfrak{a}_2 \equiv 0 \pmod{\mathfrak{a}}.$$

Andererseits ist aber nach der Voraussetzung $\mathfrak{p} \equiv 0 \pmod{\mathfrak{a}_2^2}$; daraus folgt

$$(4) \quad \mathfrak{a}_2 = \mathfrak{a}'_2 = \mathfrak{a}_2^2.$$

Wäre $\mathfrak{a}_2$ vom Einheitsideal verschieden, so würde

$$\mathfrak{o} = \mathfrak{h} + \mathfrak{a}_2, \quad \mathfrak{h} \not\equiv (0), \quad \mathfrak{p} \not\equiv \mathfrak{a}_2, \quad \mathfrak{p} \equiv 0 \pmod{\mathfrak{a}_2}.$$

Folglich hätten wir den Widerspruch, dass für zwei Elemente $\mathfrak{h}$, $\mathfrak{a}_2$ aus $\mathfrak{h}$ und $\mathfrak{a}_2$, die beiden unteilbar durch $\mathfrak{p}$ sind, $\mathfrak{h}\mathfrak{a}_2 \equiv 0 \pmod{\mathfrak{p}}$ ist.

Daraus folgt wegen (3), (4)

$$\mathfrak{o} = \mathfrak{a}_2 = \mathfrak{a}, \quad \mathfrak{o} = \mathfrak{o}^2.$$

Damit soll der Ring $\Re$ das Einheitselement e enthalten.⁽¹⁾

Gibt es ein Ideal zwischen $\mathfrak{o}$ und $\mathfrak{p}$, so existiert ein Ideal $\mathfrak{b} = (\mathfrak{p}, (ra')) \not\equiv \mathfrak{o}$, das ein echter Teiler von $\mathfrak{p}$ ist, da $\mathfrak{o} = \mathfrak{a}_2 = (\mathfrak{p}, (a'))$ ist. Auf gleiche Weise können wir damit zeigen, dass $\mathfrak{p} = \mathfrak{p}^2$ oder $\mathfrak{o} = \mathfrak{b}$ ist. Der zweite Fall ist aber unmöglich. Falls $\mathfrak{p} \not\equiv \mathfrak{p}^2$, so wird $\mathfrak{p}$ hiermit ein maximales Primideal, und $\Re$ muss das Einheitselement enthalten.

Umgekehrt ist die Bedingung auch offenbar hinreichend; womit die Behauptung bewiesen ist.

Satz 4. *Ist ein Primideal $\mathfrak{p}_1$ ein Teiler eines Primideals $\mathfrak{p}$, und ist $\mathfrak{p}_1$ vom Einheitsideal verschieden, und ist ferner*

(1) Aus Satz 1 folgt unmittelbar, dass in $\Re$ das Einheitselement e existiert, wenn $\mathfrak{o} = \mathfrak{o}^2$ ist.

$$\mathfrak{d} = [\mathfrak{p}_1^m, \mathfrak{p}] = \mathfrak{p}_1^m \mathfrak{p},$$

so existiert ein durch $\mathfrak{p}$ unteilbares Element h von der Art, dass

$$\mathfrak{p}^m \cdot h = (0) \quad .^{(1)}$$

Aus Satz 2 folgt die Existenz eines durch $\mathfrak{p}_1^m$ teilbaren Elementes p_1 von der Eigenschaft, dass für jedes Element d aus $\mathfrak{d}$ stets $dp_1 = d$ ist, und folglich wird $p_1^2 p = p_1 p$ für jedes Element p aus $\mathfrak{p}$, da $\mathfrak{d} = \mathfrak{p}_1^m \mathfrak{p}$ ist. Daraus folgt

$$(1) \quad (p_1^2 - p_1) \cdot \mathfrak{p} = (0) .$$

Wenn $p_1^2 - p_1 \equiv 0 \pmod{\mathfrak{p}}$ ist, so wird wegen $\mathfrak{d} \pmod{p_1} = \mathfrak{d}$, $p_1^2 - p_1 \equiv 0 \pmod{\mathfrak{d}}$

$$\mathfrak{d}_1 = (\mathfrak{d}, (p_1)) = (\mathfrak{d}, (p_1^2)) = (\mathfrak{d}, (p_1))^2 = \mathfrak{d}_1^2 .$$

Da $\mathfrak{p}_1^m$ vom Einheitsideal verschieden ist, so ist $\mathfrak{d}_1$ auch vom Einheitsideal verschieden, und ferner wird wegen $\mathfrak{d}_1^2 = \mathfrak{d}_1$

$$\mathfrak{o} = \mathfrak{h} + \mathfrak{d}_1, \quad \mathfrak{d}_1 \equiv 0 \pmod{\mathfrak{p}_1^m},$$

wo $\mathfrak{h}$ von (0) verschieden ist. Andererseits ist aber

$$\mathfrak{p}^m \equiv 0 \pmod{\mathfrak{d}_1},$$

da $\mathfrak{p}^m \equiv 0 \pmod{\mathfrak{d}}$ ist. Da $\mathfrak{p}_1$ von $\mathfrak{o}$ verschieden ist, so soll $\mathfrak{h} \not\equiv 0 \pmod{p_1}$ sein. Daraus folgt, dass für ein Element h aus $\mathfrak{h}$

$$h \not\equiv 0 \pmod{\mathfrak{p}}, \quad h \cdot \mathfrak{p}^m = (0)$$

ist.

Wenn $p_1^2 - p_1 \not\equiv 0 \pmod{\mathfrak{p}}$ ist, so setzen wir $h = p_1^2 - p_1$. Dann folgt offenbar aus (1)

$$h \not\equiv 0 \pmod{\mathfrak{p}}, \quad h \mathfrak{p}^m = (0);$$

womit der Satz bewiesen ist.

Mit Hilfe des obigen Beweises ergibt sich leicht

Zusatz. Ist $\mathfrak{p}$ ein von $\mathfrak{o}$ verschiedenes Primideal, und ist

$$\mathfrak{d} = [\mathfrak{p}, \mathfrak{o}^m] = \mathfrak{p} \cdot \mathfrak{o}^m,$$

(1) Der Satz gilt auch, falls $\mathfrak{p}$ und $\mathfrak{p}_1$ nicht prim sind.

so gibt es ein durch $\mathfrak{p}$ unteilbares Element r , für das $r \mathfrak{p}^m = (0)$ ist, oder wird für eine passende Zahl λ

$$\mathfrak{o} = \mathfrak{h} + \mathfrak{o}^m, \quad \mathfrak{h}^\lambda = (0), \quad \mathfrak{o}^{2m} = \mathfrak{o}^m.$$

Es gibt ein Element r_1 , so dass

$$(r_1^2 - r_1)\mathfrak{p} = (0), \quad r_1 \equiv 0 \pmod{\mathfrak{o}^m}, \quad r_1 \mathfrak{d} = \mathfrak{d}.$$

Falls $r_1^2 - r_1 \equiv 0 \pmod{\mathfrak{p}}$, so wird

$$\mathfrak{o} = \mathfrak{h} + \mathfrak{d}_1, \quad \mathfrak{d}_1^2 = \mathfrak{d}_1, \quad \mathfrak{d}_1 = (\mathfrak{d}, (r_1)) \equiv 0 \pmod{\mathfrak{o}^m}, \quad \mathfrak{p}^m \equiv 0 \pmod{\mathfrak{d}}.$$

Ist $\mathfrak{d}_1 \equiv 0 \pmod{\mathfrak{p}}$, so existiert damit ein Element r ausserhalb $\mathfrak{p}$, für das $r \mathfrak{p}^m = (0)$. Ist $\mathfrak{h} \equiv 0 \pmod{\mathfrak{p}}$, so ist $\mathfrak{h}$ ein nilpotentes Ideal, da $\mathfrak{p}^m \equiv 0 \pmod{\mathfrak{d}_1}$ ist. Ferner wird $\mathfrak{o}^m = \mathfrak{d}_1$.

Falls $r_1^2 - r_1 \not\equiv 0 \pmod{\mathfrak{p}}$ ist, so ist die Behauptung auch richtig.

Satz 5. Ist $\mathfrak{p}$ ein maximales Primideal aus dem Ring $\mathfrak{R}$ mit Einheitselement, so ist jeder Teiler von einer Potenz von $\mathfrak{p}$ primär.

Zunächst zeigen wir, dass $\mathfrak{p}$ ein maximales Ideal ist. Ist $\mathfrak{a}$ ein von $\mathfrak{o}$ verschiedenes Ideal, das ein echter Teiler von $\mathfrak{p}$ ist, so wird $\mathfrak{a}$ nach der Voraussetzung kein Primideal. Damit können wir ein Element r finden, so dass

$$r \not\equiv 0 \pmod{\mathfrak{a}}, \quad \mathfrak{o}r \equiv 0 \pmod{\mathfrak{a}}.$$

Das ist aber unmöglich, da $\mathfrak{R}$ das Einheitselement besitzt. Hiermit soll $\mathfrak{p}$ zugleich ein maximales Ideal sein.

Ist ein Ideal $\mathfrak{q}$, das ein Teiler von $\mathfrak{p}^\lambda$ ist, nicht primär, so können wir wegen $\mathfrak{q} \equiv 0 \pmod{\mathfrak{p}}$ zwei Elemente r, p auswählen, so dass

$$(1) \quad r \mathfrak{p} \equiv 0 \pmod{\mathfrak{q}}, \quad r \not\equiv 0 \pmod{\mathfrak{p}}, \quad p \not\equiv 0 \pmod{\mathfrak{q}}.$$

Ferner können wir ein Element p' finden, so dass

$$(2) \quad \mathfrak{p} p p' \equiv 0 \pmod{\mathfrak{q}}, \quad p p' \not\equiv 0 \pmod{\mathfrak{q}}.$$

Da $\mathfrak{p}$ ein maximales Ideal ist, so wird $\mathfrak{o} = (\mathfrak{o}r, \mathfrak{p})$, und folglich wird für das Einheitselement e

$$(3) \quad e = r r' + p'', \quad r' \not\equiv 0 \pmod{\mathfrak{p}}, \quad p'' \equiv 0 \pmod{\mathfrak{p}}.$$

Aus (I) und (3) folgt

$$r r' p p' = (e - p'') p p' \equiv 0 \pmod{\mathfrak{q}}.$$

Wegen (2) wird hiermit

$$pp' = epp' \equiv 0 \pmod{q}$$

gegen die Voraussetzung. Hiermit ist der Satz vollständig bewiesen.

§ 3. Bedingung für die Darstellbarkeit jedes Ideals als Produkt von grössten Primäridealen.

Zunächst sollen Ringe mit Einheitsselement untersucht werden.

Satz 6. *Damit im kommutativen Ring $\mathfrak{R}$ mit Einheitsselement stets*

$$a = [q_1, q_2, \dots, q_n] = q_1 \cdot q_2 \cdot \dots \cdot q_n$$

ist, wo $[q_1, \dots, q_n]$ eine kürzeste Darstellung von a durch grösste Primärideale bedeutet, ist notwendig und hinreichend, dass $\mathfrak{o} = \mathfrak{o}_1 + \mathfrak{o}_2 + \dots + \mathfrak{o}_m$ ist, wobei $\mathfrak{o}_i$ die Ideale aus $\mathfrak{o}$ von den folgenden Eigenschaften sind:

1. *$\mathfrak{o}_i$ sind direkt-unzerlegbar und besitzen Einheitsselement.*
2. *In jedem Ring $\mathfrak{o}_i$ gibt es höchstens nur ein nicht-maximales Primideal $\mathfrak{p}'_i (\neq \mathfrak{o}_i)$, für das $\mathfrak{p}'_i{}^2 = (0)$ ist.*
3. *Ist $\mathfrak{p}'_i$ nicht Nullideal, so ist $\mathfrak{p}'_i$ direkte Summe von minimalen Idealen $\mathfrak{m}_{ij}$; dabei sind $\mathfrak{m}_{ij} = (0) : \mathfrak{p}_{ij}$ für maximale Primideale $\mathfrak{p}_{ij}$ aus $\mathfrak{o}_i$, und $\mathfrak{p}_{ik}\mathfrak{m}_{ij} = \mathfrak{m}_{ij} (k \neq j)$ für jedes maximale Primideal $\mathfrak{p}_{ik} (\neq \mathfrak{p}_{ij})$ aus $\mathfrak{o}_i$.*

Zunächst nehmen wir an, dass für jede kürzeste Darstellung $a = [q_1, \dots, q_n]$ durch grösste Primärideale stets $a = q_1 \cdot \dots \cdot q_n$ ist.

Nach dem Teilerkettensatz wird $\mathfrak{R}$ direkte Summe von endlich vielen direkt-unzerlegbaren Idealen $\mathfrak{o}_i$ aus $\mathfrak{R}$, und ferner sind $\mathfrak{o}_i^2 = \mathfrak{o}_i$, da $\mathfrak{R}$ das Einheitsselement enthält. Nämlich wird

$$(1) \quad \mathfrak{o} = \mathfrak{o}_1 + \mathfrak{o}_2 + \dots + \mathfrak{o}_m.$$

Ist jedes Primideal maximal, so ist der Satz einleuchtend.

Es sei $\mathfrak{p}$ ein nicht-maximales Primideal aus $\mathfrak{R}$. Ist $\mathfrak{p} = \mathfrak{p}^2$, so wird $\mathfrak{p}$ kein echter Teiler eines anderen Primideals. Im anderen Falle ist $\mathfrak{p}$ nach Satz 3 unteilbar durch eine Potenz $\mathfrak{b}_1^{\lambda_1}$ eines Ideals $\mathfrak{b}_1$, das ein echter Teiler von $\mathfrak{p}$ ist. Es sei jetzt

$$\mathfrak{b}_1^{\lambda_1} = [q'_1, \dots, q'_{k_1}]$$

eine kürzeste Darstellung durch grösste Primärideale, dann ist $\mathfrak{p}$ unteilbar durch wenigstens eines, etwa q'_1 , aus q'_i ; nämlich wird

$$\mathfrak{p} \not\equiv 0 \pmod{q'_1}.$$

Ist p_1 das zu q'_i gehörige Primideal, so ist p_1 ein von 0 verschiedener echter Teiler von p , da $p \equiv 0(b_1)$ ist, und ferner ist $p_1^2 \neq p_1$. Ist p_1 noch nicht maximales Primideal, so ist p_1 unteilbar durch eine Potenz $b_2^{\lambda_2}$ eines Ideals b_2 , das echter Teiler von p_1 ist, und weiter erhalten wir auch

$$b_2^{\lambda_2} = [q''_1, \dots, q''_{k_2}].$$

Damit ist p_1 durch etwa q''_1 unteilbar, und das zu q''_1 gehörige Primideal p_2 ist ein echter Teiler von p_1 und wird $p_2^2 \neq p_2$. Nach einer endlichen Anzahl von Schritten des Verfahrens ist p_i endlich ein maximales Primideal, und p_{i-1} ist teilbar durch p_i , aber nicht durch p_i^ρ , dabei ist ρ eine passende Zahl. Da p_i ein maximales Primideal ist, so wird p_i^ρ nach Satz 5 ein zu p_i gehöriges Primärideal. Nach der Voraussetzung ist

$$\mathfrak{d} = [p_{i-1}, p_i^\rho] = p_{i-1} \cdot p_i^\rho.$$

Wegen Satzes 4 existiert ein durch p_{i-1} unteilbares Element h derart, dass $hp_{i-1}^\rho = (0)$ ist. Hiermit ist p_{i-1} kein echter Teiler von Primideal; also ist p nur durch maximales Primideal teilbar. Zusammenfassend ist jedes Primideal, das durch ein maximales Primideal echt teilbar ist, kein Teiler von anderem Primideal.

Ist $p = p^2$, so wird aus (I)

$$p = v_1 + \dots + v_{i-1} + v_{i+1} + \dots + v_m,$$

und in v_i ist (0) das einzige Primideal, das durch maximales Primideal aus v_i teilbar ist.

Im anderen Falle wird $\mathfrak{d}_1 = [p, p_1^\rho] = p \cdot p_1^\rho$, wo p_1 ein maximales Primideal ist. Nach Satz 2 gibt es in p_1^ρ ein Element p_1 , derart, dass für jedes Element d_1 aus $\mathfrak{d}_1$ $d_1 p_1 = d_1$ ist. Ist e das Einheitselement aus $\mathfrak{R}$, so wird für jedes Element d_1 aus $\mathfrak{d}_1$

$$(p_1 - e)d_1 = 0, \quad p_1 - e \neq 0 \ (p_1).$$

Aus $\mathfrak{d}_1 \cdot (p_1 - e) = p_1^\rho \cdot p \cdot (p_1 - e) = (0)$ folgt ferner die Existenz eines Elementes p' von der Eigenschaft, dass

$$p_1 \cdot p' = (0) \quad p' \neq 0.$$

Denn, da p_1^ρ ein Primärideal und $p \neq 0(b_1)$ ist, so soll $p(p_1 - e) \neq (0)$ sein. Es sei nun $m_1 = (0) : p_1^\rho$, dann ist m_1 vom Nullideal verschieden, und ferner wird

$$[m_1, d_1] = (0), \quad m_1 \equiv 0 \ (p),$$

da $p_1 d_1 = d_1$ und p_1 ein maximales Primideal ist. Ist p'' ein beliebiges Element aus p , so wird $p_1'(p_1 p'' - p'') = (0)$, da $p_1' p'' \equiv 0(d_1)$ ist. Daraus folgt wegen $m_1 \equiv 0(p)$, $p \cdot p_1' = d_1$

$$(2) \quad p = m_1 + d_1,$$

und m_1 ist nilpotent. Ferner soll m_1 ein minimales Ideal und $m_1 = (0):p_1$ sein. Sonst würde für ein echtes Vielfaches $m_1' (\neq (0))$ von m_1 , das durch $(0):p_1 \neq (0)$ teilbar ist⁽¹⁾

$$(m_1', d_1) = [p, q'], \quad q' = (m_1', p_1'),$$

wo q' wegen Satzes 5 das zu p_1 gehörige Primärideal ist, und die Darstellung eine kürzeste ist. Aus der Voraussetzung würde $(m_1', d_1) = p q' = d_1$ mit Widerspruch, da $p_1 m_1' = (0)$ ist.

Ist $d_1 = d_1^2$, so folgt aus der Eigenschaft von Primideal p und (I)

$$d_1 = o_1 + \dots + o_{i-1} + o_{i+1} + \dots + o_m, \quad m_1 = [o_i, p],$$

und ferner ist m_1 ein einziges nicht-maximales Primideal aus o_i und $m_1^2 = (0)$. Weiter wird $p_1 = (0):m_1$, und für jedes von p_1 verschiedene maximale Primideal p_j aus o ist $m_1 p_j = m_1$; sonst würde $o m_1 = (0)$ mit Widerspruch.

Ist $d_1^2 \neq d_1$, so wird

$$d_1^2 = [p, q_1, \dots, q_l].$$

Denn aus $p_1 m_1 = (0)$, $(p_1 - e) d_1 = (0)$ folgt, dass kein Primärideal zwischen p und d_1^2 existiert. Ferner wegen $p_1 = d_1^2:m_1$ ist p_1 ein zugehöriges Primideal; damit ist q_1 ein zu p_1 gehöriges Primärideal. Für jedes n ist stets $d_1 \equiv 0(p_1^n)$, und folglich wird $d_1^2 \neq [p, q_1]$. Hiermit wird für das zu q_2 gehörige Primideal p_2 , das ein Teiler von p ist,

(1) Ist d ein gemeinsames Element von p und q' , so wird

$$d = m_1 + d_1 = m_1' + p_1',$$

wo m_1, d_1, m_1', p_1' die Elemente aus $m_1, d_1, m_1', p_1 p_1$ sind. Daraus folgt

$$m_1 - m_1' = p_1' - d_1, \quad m_1 - m_1' \equiv 0(p), \quad p_1' - d_1 \equiv 0(p_1 p_1),$$

also wird $m_1 - m_1' = p_1' - d_1 \equiv 0(d_1), \quad m_1 - m_1' \equiv 0(m_1).$

Damit wird $m_1 = m_1', \quad p_1' = d_1$. Nämlich ist $[p, q'] \equiv 0((m_1', d_1))$. Umgekehrt ist auch $(m_1', d_1) \equiv 0([p, q'])$.

$p \neq [p, p_2^2] = d_2$, wo p_2 eine passend grosse Zahl bedeutet. Auf gleiche Weise können wir damit zeigen, dass

$$(3) \quad p = m_2 + d_2, \quad m_2^2 = (0), \quad p_2 = (0) : m_2, \quad m_2 = (0) : p_2,$$

und m_2 ein minimales Ideal ist. Aus (2) und (3) folgt

$$p = m_1 + d_1 = m_2 + d_2.$$

Durch Multiplikation mit p_1 und p_2 erhalten wir

$$d_1 = p_1(m_2 + d_2), \quad d_2 = p_2(m_1 + d_1).$$

Da $p_1 m_2 \neq (0)$, $p_2 m_1 \neq (0)$ ist, so folgt daraus

$$d_1 = m_2 + p_1 d_2, \quad d_2 = m_1 + p_2 d_1.$$

Nämlich wird

$$(4) \quad p = m_1 + m_2 + d_{12}, \quad d_{12} = [d_1, d_2] = p_1 d_2 = p_2 d_1.$$

Denn, da für ein Element p_1 aus p_1^2 stets $d_1 p_1 = d_1$ ist, wo d_1 ein beliebiges Element aus d_1 bedeutet, so ist

$$p_1 d_2 = p_1(m_1 + p_2 d_1) = p_1 p_2 d_1 = p_2 d_1,$$

und für ein Element d_{12} aus d_{12} wird

$$(d_{12}) = (d_1) = (d_2), \quad p_1 d_{12} = (d_1) = p_1 d_2,$$

daraus folgt

$$d_{12} \equiv 0 \pmod{p_1 d_2};$$

also wird

$$d_{12} = p_1 d_2 = p_2 d_1.$$

Wenn $d_{12} = d_{12}^2$ ist, so wird

$$d_{12} = v_1 + \dots + v_{i-1} + v_{i+1} + \dots + v_m, \quad m_1 + m_2 = [v_i, p].$$

Im anderen Falle wird wieder wegen $m_1 p_1 = (0)$, $m_2 p_2 = (0)$, $d_{12}(p_1 - e) = (0)$

$$d_{12}^2 = [p, q'_1, q'_2, \dots, q'_l],$$

dabei ist q'_1 bzw. q'_2 das zu p_1 bzw. p_2 gehörige Primideal, und $d_{12}^2 \neq [p, q'_1, q'_2]$. Hiermit existiert in der Darstellung ein Primärkomponent, das zu einem von p_1, p_2 verschiedenen maximalen Primideal p_3 gehört, und daraus folgt

$$(5) \quad \mathfrak{d}_3 = [\mathfrak{p}, \mathfrak{p}_3^2], \quad \mathfrak{p} = \mathfrak{m}_3 + \mathfrak{d}_3, \quad \mathfrak{m}_3^2 = (0), \quad \mathfrak{d}_3 \mathfrak{p}_3 = \mathfrak{d}_3, \quad \mathfrak{m}_3 = (0) : \mathfrak{p}_3.$$

Aus (4), (5) folgt $\mathfrak{p} = \mathfrak{m}_1 + \mathfrak{m}_2 + \mathfrak{d}_{12} = \mathfrak{m}_3 + \mathfrak{d}_3$. Durch Multiplikation mit $\mathfrak{p}_1 \mathfrak{p}_2$, $\mathfrak{p}_3$ erhalten wir

$$\mathfrak{d}_3 = \mathfrak{m}_1 + \mathfrak{m}_2 + \mathfrak{p}_3 \mathfrak{d}_{12}, \quad \mathfrak{d}_{12} = \mathfrak{m}_3 + \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{d}_3,$$

oder

$$\mathfrak{p} = \mathfrak{m}_1 + \mathfrak{m}_2 + \mathfrak{m}_3 + \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{d}_3, \quad \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{d}_3 = \mathfrak{p}_3 \mathfrak{d}_{12} = [\mathfrak{d}_1, \mathfrak{d}_2, \mathfrak{d}_3].$$

Damit erhalten wir

$$\mathfrak{p} = \mathfrak{m}_1 + \mathfrak{m}_2 + \mathfrak{m}_3 + \mathfrak{d}_{123}, \quad \mathfrak{d}_{123} = [\mathfrak{d}_1, \mathfrak{d}_2, \mathfrak{d}_3].$$

Falls noch nicht $\mathfrak{d}_{123}^2 = \mathfrak{d}_{123}$ ist, so finden wir in derselben Weise eine Darstellung

$$\mathfrak{p} = \mathfrak{m}_1 + \dots + \mathfrak{m}_4 + \mathfrak{d}_{1234},$$

und indem wir eine endliche Anzahl von Malen fortfahren, gelangen wir zu einem Schluss, da für jedes $\mathfrak{m}_i$ $\mathfrak{m}_i \not\equiv 0 \pmod{(\mathfrak{m}_1 + \dots + \mathfrak{m}_{i-1} + \mathfrak{m}_{i+1} + \dots)}$ ist. Nämlich erhalten wir endlich

$$\mathfrak{p} = \mathfrak{m}_1 + \dots + \mathfrak{m}_s + \mathfrak{d}_{12\dots s}, \quad \mathfrak{m}_i^2 = (0), \quad \mathfrak{d}_{12\dots s}^2 = \mathfrak{d}_{12\dots s},$$

und $\mathfrak{m}_i$ ist ein minimales Ideal. Da $\mathfrak{o}_i$ direkt-unzerlegbar ist, so soll

$$[\mathfrak{o}_i, \mathfrak{p}] = \mathfrak{m}_1 + \mathfrak{m}_2 + \dots + \mathfrak{m}_s$$

sein, und $\mathfrak{m}_1 + \dots + \mathfrak{m}_s$ ist ein einziges nicht-maximales Primideal aus $\mathfrak{o}_i$ und $(\mathfrak{m}_1 + \dots + \mathfrak{m}_s)^2 = (0)$. Hiermit sind die Bedingungen notwendig.

Umgekehrt behaupten wir, dass die Bedingungen auch hinreichend sind. Es sei nämlich $\mathfrak{o} = \mathfrak{o}_1 + \mathfrak{o}_2 + \dots + \mathfrak{o}_m$ die direkte Summe der Ideale $\mathfrak{o}_i$, die die im Satz ausgesprochenen Eigenschaften besitzen. Es sei auch α ein nicht-primäres Ideal, und sei

$$\alpha = [\mathfrak{q}_1, \dots, \mathfrak{q}_n]$$

eine kürzeste Darstellung durch grösste Primärideale. Sind alle zugehörigen Primideale die höchsten Primideale von α , so wird

$$\alpha = \mathfrak{q}_1 \cdot \mathfrak{q}_2 \cdot \dots \cdot \mathfrak{q}_n.$$

Denn aus der Voraussetzung folgt

$$\mathfrak{q}_i = \mathfrak{o}_1 + \dots + \mathfrak{o}_{i-1} + \mathfrak{q}'_i + \mathfrak{o}_{i+1} + \dots + \mathfrak{o}_m,$$

wo q'_i ein Primärideal aus v_i ist. Ist das zu q'_i gehörige Primideal aus v_i nicht maximal, so wird $v_i \equiv 0 (q_j)$ ($j = 1, \dots, i-1, i+1, \dots, n$). Damit wird $(q_i, q_j) = v$. Ist das zu q'_i gehörige Primideal maximal, so wird auch $(q_i, q_j) = v$. Damit wird $\alpha = [q_1, \dots, q_n] = q_1 q_2 \dots q_n$.⁽¹⁾

Im anderen Falle seien die zugehörigen Primideale $p_1, \dots, p_k$ die höchsten Primideale von α ; dann werden $p_{k+1}, \dots, p_n$ die zugehörigen maximalen Primideale, die Teiler eines aus $p_1, \dots, p_k$ sind, und für jedes nicht-maximale zugehörige Primideal p_i wird $p_i = q_i$. Es seien $p_{k+1}, \dots, p_{k+l}$ die zugehörigen nicht-höchsten Primideale von α , für die $m_i = (0) : p_{k+i}$ durch α unteilbar ist, und seien auch $p_{k+l+1}, \dots, p_n$ die zugehörigen nicht-höchsten Primideale, für die $(0) : p_{k+i}$ durch α teilbar ist. Ist $m_i = (0) : p_{k+i}$, $m_i \equiv 0 (\alpha)$, so wird nach den Eigenschaften 3 für jedes durch α unteilbare Element p_i aus $p_i p_{k+i} \equiv 0 (\alpha)$, da ein nicht-maximales zugehöriges Primideal p_i durch p_{k+i} teilbar ist. Damit ist p_{k+i} kein zu α gehöriges Primideal mit Widerspruch. Damit wird $k+l = n$. Setzen wir nun $\delta = [q_1, \dots, q_k]$, so wird offenbar

$$\delta = q_1 q_2 \dots q_k, \quad \alpha \equiv 0 (\delta),$$

und ferner ist $\alpha p_{k+1} \dots p_n = \alpha$.⁽²⁾ Daraus folgt $\alpha q_{k+1} \dots q_n = \alpha$,

$$\alpha \equiv 0 \quad (\delta q_{k+1} \dots q_n = q_1 \dots q_k \dots q_n).$$

Damit wird $\alpha = q_1 \dots q_k \dots q_n$; womit der Satz bewiesen ist.

Es soll jetzt derselbe Satz für Ring ohne Einheitsselement untersucht werden.

Satz 7. *Damit in einem kommutativen Ringe $\mathfrak{R}$ ohne Einheitsselement stets*

$$\alpha = [q_1, \dots, q_n] = q_1 \dots q_n$$

ist, ist notwendig und hinreichend, dass $\mathfrak{R}$ höchstens nur ein maximales Primideal $\mathfrak{p}$ hat, und dass, falls $\mathfrak{p} \neq (0)$, das Primideal $\mathfrak{p}$ die folgenden Eigenschaften besitzt :

$$1. \quad \mathfrak{p} = \mathfrak{n} + \delta, \quad \mathfrak{o}\mathfrak{n} = (0), \quad \mathfrak{o}\delta' = \delta'$$

für jedes Vielfache δ' von δ .

(1) E. Noether, Idealtheorie in Ringbereichen, Math. Annalen, **83**, § 8.

(2) Ist für das maximale Primideal $p_{is} = [v_i, p_{k+s}]$ aus v_i $m_i = (0) : p_{is}$, so ist m_i eines aus m_{ij} in $p_i' = m_{i1} + \dots + m_{in}$. Denn, da $m_i \equiv 0 (\alpha)$ ist, so soll $m_i \neq (0)$ sein. Aus $p_i' \equiv 0 (p_{is})$ folgt $m_i \equiv 0 (p_i')$. Da $m_{ij} = (0) : p_{ij}$ ($j = 1, \dots, n$) ist, so wird $m_i p_{i1} \dots p_{in} = (0)$; also $p_{i1} \dots p_{in} \equiv 0 (p_{is})$. Hiermit wird etwa $p_{is} = p_{in}$; daraus folgt $m_i = m_{in}$. Daher folgt die obige Beziehung.

2. $\mathfrak{n}$ ist ein minimales primäres Ideal, und es gibt kein Primideal ausser $\mathfrak{o}$, $\mathfrak{p}$ und $\mathfrak{n}$.⁽¹⁾

Die Bedingung ist notwendig. Es sei nämlich $\mathfrak{p}$ ein maximales Primideal. Gibt es kein maximales Primideal, so ist der Satz einleuchtend.

Ist $\mathfrak{p} = \mathfrak{p}^2$, so wird

$$\mathfrak{o} = \mathfrak{m} + \mathfrak{o}_1 + \dots + \mathfrak{o}_m, \quad \mathfrak{p} = \mathfrak{o}_1 + \dots + \mathfrak{o}_m,$$

wo $\mathfrak{m}$ und $\mathfrak{o}_i$ direkt-unzerlegbar sind, und in $\mathfrak{m}$ gibt es keinen Nullteiler. Es sei nun $m \geq 1$. Ist $\mathfrak{m}' (\neq (0))$ ein echtes Vielfaches von $\mathfrak{m}$, so wird $\mathfrak{m}'$ ein Primärideal aus $\mathfrak{m}$. In der Darstellung $\mathfrak{m}' = [\mathfrak{q}_1, \dots, \mathfrak{q}_l]$ sind

$$\mathfrak{q}_1 = \mathfrak{m}' + \mathfrak{o}_1 + \dots + \mathfrak{o}_m, \quad \mathfrak{m} \equiv 0 \pmod{\mathfrak{q}_i} \quad (i = 2, \dots, l), \quad (l \geq 2).$$

Aus der Voraussetzung folgt $\mathfrak{m}' = \mathfrak{m}^{l-1}\mathfrak{m}'$. Da für eine hinreichend grosse Zahl ρ $\mathfrak{m}^\rho \equiv 0 \pmod{\mathfrak{m}'}$ ist, so wird $\mathfrak{m}' = \mathfrak{m}'^2$. Also wird $\mathfrak{m}$ direkt-unzerlegbar mit Widerspruch. Hiermit soll $\mathfrak{m}$ ein Körper sein. Das ist aber unmöglich. Damit ist $\mathfrak{o} = \mathfrak{m}$, $\mathfrak{p} = \mathfrak{p}^2 = (0)$. In $\mathfrak{R}$ gibt es hiermit kein von $\mathfrak{o}$ und (0) verschiedenes Primideal.

Im anderen Falle ist $\mathfrak{p}$ unteilbar durch eine Potenz $\mathfrak{b}^\lambda$ eines echten Teilers $\mathfrak{b}$ von $\mathfrak{p}$. Da $\mathfrak{p}$ ein maximales Primideal ist, so wird $\mathfrak{b}^\lambda = \mathfrak{q}$ ein zu $\mathfrak{o}$ gehöriges Primärideal. Aus der Voraussetzung folgt damit

$$(1) \quad \mathfrak{b} = [\mathfrak{p}, \mathfrak{q}] = \mathfrak{p} \cdot \mathfrak{q}, \quad \mathfrak{q} \neq (0).$$

Aus Satz 2 folgt damit die Existenz eines durch $\mathfrak{q}$ teilbaren Elementes $q (\neq 0)$, für das stets

$$dq = \dot{d}$$

ist, wo d ein beliebiges Element aus $\mathfrak{b}$ bedeutet. Da $\mathfrak{p} \cdot \mathfrak{q} \equiv 0 \pmod{\mathfrak{b}}$ ist, so wird $p'q^2 = p'q$ für jedes Element p' aus $\mathfrak{p}$. Wäre für jedes Element p' aus $\mathfrak{p}$ stets $p'q - p' = 0$, so würde $\mathfrak{p} \equiv 0 \pmod{\mathfrak{q}}$ mit Widerspruch. Damit ist für ein Element p aus $\mathfrak{p}$

$$pq - p \neq 0, \quad q(pq - p) = 0.$$

Die Gesamtheit $\mathfrak{n}$ der Elemente n aus $\mathfrak{p}$, für die $nq = 0$ ist, bildet ein Ideal und ist vom Nullideal verschieden, und ferner wird $[\mathfrak{n}, \mathfrak{b}] = (0)$. Ist p' ein beliebiges Element aus $\mathfrak{p}$, so wird $q(p'q - p') = 0$, und folglich wird

$$p'q - p' \equiv 0 \pmod{\mathfrak{n}}, \quad p'q \equiv 0 \pmod{\mathfrak{b}}.$$

(1) Ich habe noch keine Antwort auf die Frage: ob $\mathfrak{n}$ prim sein kann.

Daraus folgt wegen $p^{\lambda+1} \equiv 0 \pmod{\mathfrak{d}}$

$$(2) \quad p = n + \mathfrak{d}, \quad n^{\lambda+1} = (0).$$

Da nach (2) $[n, q] = (0)$ ist, so wird

$$(3) \quad nq = (0).$$

Damit ist $n' = (0) : \mathfrak{o}$ vom Nullideal verschieden. Wäre $n' \neq n$, so würde

$$n' + \mathfrak{d} = [p, q'], \quad q' = n' + q.$$

Aus $n'p = (0)$ folgte aber $pq' \neq n' + \mathfrak{d}$ gegen die Voraussetzung. Hiermit erhalten wir

$$(4) \quad p = n + \mathfrak{d}, \quad \mathfrak{o}n = (0), \quad \mathfrak{o}\mathfrak{d}' = \mathfrak{d}',$$

für jedes Vielfache $\mathfrak{d}'$ von $\mathfrak{d}$, und ferner ist n ein minimales Ideal. Gibt es ein nicht-primäres Ideal α zwischen n und p (einschl. n), so ist ein zu α gehöriges Primideal p_1 durch p teilbar, und in der Darstellung $\alpha = [q_1, \dots, q_l]$ ist damit

$$q_1 = n + \mathfrak{d}',$$

wo $\mathfrak{d}'$ ein Vielfaches von $\mathfrak{d}$ bedeutet. Aus (4) folgt aber

$$q_1 q_2 \dots q_l \equiv 0 \pmod{\mathfrak{d}'},$$

also wird $\alpha \neq q_1 \dots q_l$ gegen die Voraussetzung. Hiermit sind alle Ideale zwischen n und p primär. Da $n^2 = (0)$ und n ein minimales Ideal ist, so ist n durch jedes Primideal teilbar. In $\mathfrak{R}$ gibt es damit kein maximales Primideal ausser p , und jedes von $\mathfrak{o}$ verschiedene Primideal ist durch p teilbar.

Da $nq = (0)$, $dq = dq^2$, $q \neq 0$ für jedes Element d aus $\mathfrak{d}$ ist, so wird $p(q - q^2) = (0)$. Wir können daher zwei verschiedene Fälle unterscheiden.

1. $q - q^2 \neq 0 \pmod{p}$. Dann ist p ein einziges von $\mathfrak{o}$ verschiedenes Primideal.

2. $q - q^2 \equiv 0 \pmod{p}$. Dann wird wegen $q - q^2 \equiv 0 \pmod{q}$

$$q' = q - q^2 \equiv 0 \pmod{\mathfrak{d}},$$

also wird

$$q'^2 = (q - q^2)^2 = 0.$$

Daraus folgt, dass q' teilbar durch jedes Primideal ist. Ist $q' = 0$, so wird $q = q^2 \neq 0$. Wir erhalten damit wegen $q \equiv 0 \pmod{m}$

$$o = h + m, \quad m = m^2 \neq (0), \quad n \equiv 0 \pmod{h}, \quad h \equiv 0 \pmod{p}, \quad d \equiv 0 \pmod{m},$$

da jedes von o verschiedene Primideal teilbar durch p ist. Daraus folgt weiter $h = n$. Jedes Ideal aus m soll auch primär sein; sonst hätten wir ein nicht-primäres Ideal zwischen n und p mit Widerspruch. Aus Satz 3 folgt, dass p und n alle Primideale in $\mathfrak{R}$ sind, oder p ein einziges Primideal in o ist. Ist $q' \neq 0$, so folgt aus $q' \equiv 0 \pmod{n}$ $p \mid q' = (0)$, dass p oder o ein zu n gehöriges Primideal. Aber n ist primär, damit soll $o^p \equiv 0 \pmod{n}$, oder $p^p \equiv 0 \pmod{n}$ sein. Also ist p ein einziges von o und (0) verschiedenes Primideal und nilpotent.

Die bedingung ist auch hinreichend. Denn, wenn α nicht primär und von Null verschieden ist, so wird $\alpha = [q_1, q_2]$, und das zu q_1 bzw. q_2 gehörige Primideal ist das einzige maximale Primideal p bzw. das Einheitsideal o . Da $p = n + d$, $on = (0)$ ist, so wird $q_1 = n + d'$, wo d' ein Vielfaches von d ist. Aus $od = d$ folgt ferner $d \equiv 0 \pmod{q_2}$, und folglich wird

$$n \equiv 0 \pmod{q_2}, \quad \alpha = [q_1, q_2] = d' = q_1 q_2,$$

da $no = (0)$, $o^\lambda d' = d'$ ist. Ist α das Nullideal, so wird $\alpha = [q_1 \dots q_l] = q_1 \dots q_l$; womit der Satz bewiesen ist.