

STRUKTUR DER MULTIPLIKATIONSRINGE



Von

Shinjiro MORI

(Eingegangen am 10. 1. 1952.)

Es sei $\mathfrak{R}$ ein *kommutativer Ring*, ohne irgendwelche hinzugefügte Bedingungen vorauszusetzen. Dann heisst $\mathfrak{R}$ ein *Multiplikationsring*, wenn nur folgende Bedingung erfüllt ist :

Zu je zwei Idealen a und b aus $\mathfrak{R}$, wo $a \subset b$ ist, gibt es stets ein Ideal c in $\mathfrak{R}$, so dass $a = bc$ ist

Die vorliegende Arbeit setzt sich zum Ziel, die Strukturtheorie der Multiplikationsringe weitgehend zu entwickeln. In früherer Zeit habe ich schon einige Eigenschaften der Multiplikationsringe gewonnen,¹⁾ und diese Theorie auf Grund einiger Annahmen behandelt. Im folgenden soll nun meine Strukturtheorie noch verallgemeinert, und vertieft, und auf einem neuen, einfacheren Wege bewiesen werden.

Für die Strukturtheorie der Multiplikationsringe ist es aber von wichtiger Bedeutung die kritische Bemerkung darüber zu machen, ob in einem Multiplikationsring ein idempotentes Element in eine direkte Summe von unendlich vielen idempotenten Elementen verwandelt werden kann, welche untereinander orthogonal sind. Aus der Definition für abstrakte Ringe ergibt sich keine Aussage über die direkte Summe der unendlich vielen Elemente aus dem Orthogonalsystem von idempotenten Elementen. Sicherheit halber legen wir damit die folgende grundsätzliche Annahme vor :

Annahme. Jedes idempotentes Element lässt sich als eine direkte Summe von endlich vielen, primitiven Elementen darstellen.

Dabei bedeutet *direkte Summe* eine Summe von Elementen, die untereinander orthogonal sind, und *primitives Element* ein idempotentes, in eine direkte Summe von idempotenten Elementen unzerlegbares Element.

Um Missverständnisse zu vermeiden, mache ich hier die Aussage, dass im grundlegenden Multiplikationsring die Existenz von Einheitsselement nicht vorausgesetzt wird.

1) S. Mori, Über allgemeine Multiplikationsringe I. II. Journal of Sci. of the Hiroshima Univ. 4 (1934).

I. Die Grundlagen der Strukturtheorie.

In diesem Abschnitt beweisen wir die Sätze, welche auf dem Wege zu unserem Ziel unentbehrlich sind.

Satz I.²⁾ *Ist α ein von Null verschiedenes Ideal aus Multiplikationsring $\mathfrak{R}$ und idempotent, und ist $\mathfrak{b} \subset \alpha$ für ein Ideal $\mathfrak{b}$, so gibt es in α ein idempotentes Element, welches nicht zu $\mathfrak{b}$ gehört.*

Zunächst zeigen wir, dass es in α , aber ausserhalb von $\mathfrak{b}$, ein in bezug auf $\mathfrak{b}$ nicht nilpotentes Element a gibt. Ist $a' (= 0(\mathfrak{b}))$ ein Element aus α , so folgt nach der Definition vom Multiplikationsring $\mathfrak{R}$

$$(a') = ab' = aab' = (a')a,$$

weil a idempotent ist. Daraus ergibt sich $a' = a'a$ für ein Element a aus α , und folglich $a' = a'a^n$ für jede natürliche Zahl n . Da aber a' nicht zu $\mathfrak{b}$ gehört, so muss jede Potenz von a nicht zu $\mathfrak{b}$ gehören.

Es sei nun $\mathfrak{h}$ die Gesamtheit aller nilpotenten Elemente aus α . Dann ist $\mathfrak{h}$ durch α teilbar, aber von α verschieden, weil nach dem soeben gewonnenen Ergebnisse $a \notin \mathfrak{h}$ ist. Sei ferner m_0 die Gesamtheit aller Elemente m_0 aus α , für welche $m_0 a = 0(\mathfrak{h})$ gilt. Dann ist $\alpha \supseteq m_0 \supseteq \mathfrak{h}$, $m_0(a) \subseteq \mathfrak{h}$. Es sei dazu m die Gesamtheit aller Elemente m aus α von der Art, dass $(m)m_0 \subseteq \mathfrak{h}$ ist. Dann erhalten wir $a \in m$, $mm_0 \subseteq \mathfrak{h}$, und folglich $\alpha \supseteq m \supseteq \mathfrak{h}$. Wenn d ein gemeinsames Element von m_0 und m ist, so folgt daraus $d^2 \in \mathfrak{h}$. Da $\mathfrak{h}$ halbpriim im Bereiche des Ideals α ist, so soll danach $d \in \mathfrak{h}$ sein. Hiermit haben wir

$$(1) \quad m_0 \cap m = \mathfrak{h}.$$

Aus $(\mathfrak{h}, (a), m_0) \subseteq \alpha$ und $a = a^2$ erhalten wir auch, wie eben bewiesen, $(\mathfrak{h}, (a), m_0) = ab_0 = aab_0 = a(\mathfrak{h}, (a), m_0)$, und folglich

$$(2) \quad (\mathfrak{h}, (a)) = (\mathfrak{h}, (a), m_0)b'_0 = (\mathfrak{h}, (a), m_0)ab'_0, \quad m_0ab'_0 \subseteq (\mathfrak{h}, (a)).$$

Nach $(\mathfrak{h}, (a)) \subseteq m$ haben wir daraus $m_0ab'_0 \subseteq m$. Aus (1) folgt damit $m_0ab'_0 \subseteq \mathfrak{h}$, und weiter durch die Konstruktion von m ergibt sich $ab'_0 \subseteq m$. Nach (2) und $mm_0 \subseteq \mathfrak{h}$ ist nun damit

$$(\mathfrak{h}, (a)) = ((\mathfrak{h}, (a))m, \mathfrak{h}).$$

Für ein Element m aus m gilt danach

$$(3) \quad a \equiv am(\mathfrak{h}), \quad a(m - m^3) \equiv 0(\mathfrak{h}).$$

2) Ein halber Teil dieses Satzes ist schon in verschiedener Weise bewiesen. Vgl. S. Mori, Über allgemeine Multiplikationsringe I.

Dabei ist m nicht nilpotent in bezug auf $\mathfrak{h}$, denn a gehört nicht zu $\mathfrak{h}$. Nach unserer Definition für m , ist nun $m - m^3 \in m_0$. Ferner ist $m - m^3 \in m$ nach $m \in m$. Somit ergibt sich nach (1) endlich

$$(4) \quad m - m^3 \in \mathfrak{h}.$$

Nach diesem Resultat können wir folgendermassen die Existenz eines idempotenten Elementes beweisen. Aus (4) ergibt sich $(m - m^3)^n = 0$ für eine natürliche Zahl n , also $m^n = m^{n+1}m'$, wo m' ein Element aus m ist. Nun ist auch

$$m^n = m^{n+1}m' = m^n(mm')^2 = \dots = m^n(mm')^n.$$

Hierbei ist $m^n \neq 0(\mathfrak{h})$, denn m ist nicht nilpotent in bezug auf $\mathfrak{h}$. Setzen wir jetzt $m^n m'^n = e$, so ist $e = e^2 \notin \mathfrak{h}$, $e \in a$.

Endlich müssen wir $e \notin \mathfrak{b}$ beweisen. Wenn $e \in \mathfrak{b}$ wäre, so würde $m^n \in \mathfrak{b}$, und folglich nach (3) $a \in (\mathfrak{h}, \mathfrak{b})$. Daraus ergäbe sich $a^k \in \mathfrak{b}$, im Widerspruch zum im Anfang gewonnenen Resultat.

Damit sind die ausgesprochenen Behauptungen über die Ganzheit bewiesen.

Diesen Satz können wir auch zu dem folgenden allgemeinen Satze erweitern.

Satz 2. Sind $a \subseteq b$ und $a = ab$ für zwei Ideale a und b aus dem Multiplikationsring $\mathfrak{R}$, und ist ein Element aus a nicht nilpotent, so gibt es in b ein idempotentes Element.

Aus der Eigenschaft von $\mathfrak{R}$ folgt zunächst, dass für ein nicht nilpotentes Element a es ein Element b in $\mathfrak{b}$ gibt, so dass $a = ab$ ist. Nach $a \neq 0$ ist damit b nicht nilpotent. Ist $\mathfrak{h}$ die Gesamtheit aller nilpotenten Elemente aus $\mathfrak{b}$, so folgt daraus $a \notin \mathfrak{h}$, $b \notin \mathfrak{h}$. Andererseits gilt $a(b - b^3) = 0$ aus $a = ab$. So gehen wir schrittweise vor.

I. Wenn $b - b^3 \in \mathfrak{h}$ ist, so bekommen wir leicht, wie beim Beweise von Satz I, ein idempotentes Element aus b .

II. Im Falle $b - b^3 \notin \mathfrak{h}$, sei m die Gesamtheit aller Elemente m aus b , für welche $am = 0(\mathfrak{h})$ gilt. Dann ist $\mathfrak{b} \supseteq m \supset \mathfrak{h}$, $b - b^3 \in m$, $a \notin \mathfrak{h}$. Ferner sei m_0 die Gesamtheit aller solchen Elemente m_0 aus b , dass $(m_0)m \subseteq \mathfrak{h}$ ist. Dann ist auch

$$(1) \quad \mathfrak{b} \supseteq m_0 \supset \mathfrak{h}, \quad a \in m_0, \quad m \cap m_0 = \mathfrak{h}.$$

Nach $(a) = (a)b$ und $(a, \mathfrak{h}) = (a, \mathfrak{h}, mb)c = ((a, mb)c, \mathfrak{h})$ gilt $(a, \mathfrak{h}) = ((a, m)bc, \mathfrak{h})$ für ein Ideal c . Daraus folgt $mbc \subseteq (a, \mathfrak{h}) \subseteq m_0$, und folglich erhalten wir nach (1) $mbc \subseteq \mathfrak{h}$. Damit besteht nach der Eigenschaft von m_0 $bc \subseteq m_0$, $(a, \mathfrak{h}) = ((a)bc, \mathfrak{h})$

und daraus folgt $a \equiv ab_1(b)$, wobei b_1 ein Element aus m_0 ist. Hiermit muss $b_1 - b_1^2$ zu m und auch zu m_0 gehören. Somit wird nach (1) $b_1 - b_1^2 \equiv 0(b)$, und daraus folgt leicht die Existenz eines idempotenten Elementes in b .

2. Struktur vom nicht-idempotenten Multiplikationsring.

Mit Hilfe vorstehender Sätze lässt sich die Strukturtheorie vom Multiplikationsring $\mathfrak{R}$, für welchen $\mathfrak{R} \neq \mathfrak{R}^2$ ist, entwickeln.

Satz 3. Ist $\mathfrak{R} \neq \mathfrak{R}^2$ für den Multiplikationsring $\mathfrak{R}$, so ist jedes Ideal $(\neq (0))$ aus $\mathfrak{R}$ gleich einer endlichen Potenz von $\mathfrak{R}$.

Zum Beweise wählen wir ein Element r aus $\mathfrak{R}$ mit $r \notin \mathfrak{R}^2$. Dann soll $\mathfrak{R} = (r)$ sein. Denn wäre $\mathfrak{R} \supset (r)$, so folgte $(r) = \mathfrak{R}b \subseteq \mathfrak{R}^2$ nach der Eigenschaft vom Multiplikationsring $\mathfrak{R}$. Durch $r \notin \mathfrak{R}^2$ soll aber diese Möglichkeit ausgeschlossen sein.

Über $\mathfrak{R} = (r)$ beweisen wir noch, dass $\mathfrak{R}^n \neq \mathfrak{R}^{n+1}$ für jede natürliche Zahl n ist, wenn $\mathfrak{R}^n \neq (0)$ ist. Dazu sei m die kleinste Zahl, für welche $\mathfrak{R}^m = \mathfrak{R}^{m+1} \neq (0)$ gilt. Dann ist $\mathfrak{R}^m = \mathfrak{R}^{2m+1}$, $m \geq 2$, und daher folgt $r^m = r^{2m}r_0$ für ein Element r_0 aus $\mathfrak{R}$. Setzen wir nun $e = r^m r_0$, so ergibt sich $e = e^2 \in \mathfrak{R}^m$, $r^m = r^m e \neq 0$. Damit ist $\mathfrak{R}$ zerlegbar in die direkte Summe $\mathfrak{R} = n + \mathfrak{R}^m$, wo $n^{m-1} \neq (0)$, $n^m = (0)$ und $\mathfrak{R}^m \neq (0)$ ist. Durch unsere Annahme, dass $\mathfrak{R}$ ein Multiplikationsring ist, ergibt sich $n^{m-1} = (n^{m-1}, \mathfrak{R}^m)b$ für ein Ideal b . Da $b \subseteq \mathfrak{R}$ aber ist. So folgt daraus $n^{m-1} \subseteq (n^{m-1}, \mathfrak{R}^m)(n, \mathfrak{R}^m) = \mathfrak{R}^{2m} = \mathfrak{R}^m$, und daher wegen der direkten Summe von n und $\mathfrak{R}^m$ ergibt sich $n^{m-1} = (0)$, im Widerspruch zur Annahme von n .

Für ein beliebiges, von Null verschiedenes Ideal $a (\neq \mathfrak{R})$ können wir zwei folgende verschiedene Fälle betrachten.

1. Es sei $\mathfrak{R}^n \subseteq a$ für eine natürliche Zahl n . Wenn a gleich keiner Potenz von $\mathfrak{R}$ ist, so gilt $\mathfrak{R}^{m-1} \not\subseteq a$, $\mathfrak{R}^m \subseteq a$, $m \leq n$. Nachdem ist $(a, \mathfrak{R}^{m-1}) \supset a$, und aus der Multiplikationseigenschaft folgt

$$a = (a, \mathfrak{R}^{n-1})b \subseteq (a, \mathfrak{R}^{m-1})\mathfrak{R} \subseteq a.$$

Daher ist $a = (a\mathfrak{R}, \mathfrak{R}^m)$, $a\mathfrak{R} = (a\mathfrak{R}^2, \mathfrak{R}^{m+1})$, also sicher $a = (a\mathfrak{R}^2, \mathfrak{R}^m)$. Auf solche Weise gelangen wir endlich zur Beziehung $a = \mathfrak{R}^m$, im Widerspruch zur früher Annahme. In diesem Falle muss a damit gleich einer Potenz von $\mathfrak{R}$ sein.

II. Es stehe $\mathfrak{R}^n \not\subseteq a$ für jede natürliche Zahl n . Dann ist $\mathfrak{R}$ nicht nilpotent, und daraus folgt nach dem im vorigen Gesagten, dass jede Potenz von $\mathfrak{R}$ nicht idempotent. Wenn $a \subseteq \mathfrak{R}^m$, $a \not\subseteq \mathfrak{R}^{m+1}$ ist, so folgt nach der Multi-

likationseigenschaft ein Widerspruch $\alpha = \mathfrak{R}^m \mathfrak{b} \subseteq \mathfrak{R}^{m+1}$. Nachdem muss $\alpha \subseteq \mathfrak{R}^m$ für alle m sein. Setzen wir nun $\mathfrak{b} = \bigcap_{n=1}^{\infty} \mathfrak{R}^n$, so ergibt sich daraus $\mathfrak{b} \supseteq \alpha$. Nach den soeben gewonnenen Ergebnissen gilt $\mathfrak{b} \subseteq \mathfrak{b}$ für das Ideal $\mathfrak{b}$ mit der Eigenschaft $\mathfrak{b} = \mathfrak{R}\mathfrak{b}$, also $\mathfrak{b} = \mathfrak{R}\mathfrak{b}$, und somit

$$\mathfrak{b} = \mathfrak{R}\mathfrak{b} = \mathfrak{R}^2\mathfrak{b} = \dots = \mathfrak{b}^2 \neq (0)$$

Nach Satz I enthält damit $\mathfrak{R}$ ein idempotentes Element e . Es sei nun $\mathfrak{m}$ die Gesamtheit der durch $\mathfrak{m} = e\mathfrak{m}$ definierten Elemente $\mathfrak{m}$ und $\mathfrak{n}$ die Gesamtheit aller Elemente $\mathfrak{n}$ von der Art, dass $\mathfrak{n}e = 0$. Dann ist $\mathfrak{m} \cap \mathfrak{n} = (0)$ und $\mathfrak{m} = \mathfrak{m}^2$. Folglich ist $\mathfrak{R} \neq \mathfrak{m}$, denn $\mathfrak{R} \neq \mathfrak{R}^2$ ist. Ist r_0 ein beliebiges Element aus $\mathfrak{R}$, so ist $r_0 e = r_0 e^2$, $e(r_0 - r_0 e) = 0$. Danach ist $r_0 - r_0 e = \mathfrak{n} \in \mathfrak{n}$, $r_0 e = \mathfrak{m} \in \mathfrak{m}$ und folglich $r_0 = \mathfrak{n} + \mathfrak{m}$. Damit erhalten wir die Darstellung von $\mathfrak{R}$ in direkter Summe $\mathfrak{R} = \mathfrak{n} + \mathfrak{m}$, wo $\mathfrak{n} \neq (0)$, $\mathfrak{m} = \mathfrak{m}^2 \neq \mathfrak{R}$ ist.

Wäre für alle Elemente $\mathfrak{n}$ aus $\mathfrak{n}$ $(\mathfrak{n}) = (\mathfrak{n})\mathfrak{n}$, so würde $\mathfrak{n} = \mathfrak{n}^2$ und daraus ergäbe sich ein Widerspruch $\mathfrak{R} = \mathfrak{R}^2$. Also können wir für ein Element n_0 aus $\mathfrak{n}$ $(n_0) \supset (\mathfrak{n}_0)\mathfrak{n}$ setzen. Nach der Multiplikationseigenschaft gilt $(n_0) = (\mathfrak{n}_0, \mathfrak{m})\mathfrak{b}$ für ein Ideal $\mathfrak{b}$. Daraus folgt nach $\mathfrak{m} \cap \mathfrak{n} = (0)$, $\mathfrak{m}\mathfrak{b} = (0)$ und $\mathfrak{b} \subseteq \mathfrak{n}$. Hiermit ist $(n_0) = (\mathfrak{n}_0)\mathfrak{n}$ im Widerspruch dazu, dass $(n_0) \supset (\mathfrak{n}_0)\mathfrak{n}$ ist. Mit diesem Widerspruch ist die Richtigkeit des Satzes 3 vollständig dargetan.

Zum Schlusse dieses Abschnittes müssen wir also, auch zur Vollständigkeit der Strukturtheorie folgende selbstverständliche Bemerkung hinzufügen:

Ist jedes Ideal aus einem Ring $\mathfrak{R}$ gleich einer Potenz von $\mathfrak{R}$, so ist $\mathfrak{R}$ ein Multiplikationsring.

3. Struktur vom idempotenten Multiplikationsring.

Am Anfang stellen wir den Satz auf:

Satz 4. *Ein idempotenter Multiplikationsring $\mathfrak{R}$ erzeugt sich aus einem Orthogonalsystem von idempotenten, primitiven Elementen. D. h. $\mathfrak{R}$ lässt sich als eine direkte Summe $\mathfrak{R} = (e_\alpha) + (e_\beta) + \dots$ darstellen, wobei $(e_\alpha, e_\beta, \dots)$ ein Orthogonalsystem von idempotenten, primitiven Elementen bedeutet.*

Wenden wir Satz I auf den Ring $\mathfrak{R}$ an, so erhalten wir ein idempotentes Element e . Nach der in der Einleitung ausgesprochenen Annahme lässt sich e als eine direkte Summe von endlich vielen, idempotenten, primitiven Elementen darstellen. Es sei nun $(e_\alpha, e_\beta, \dots)$ ein maximales Orthogonalsystem von idempotenten, primitiven Elementen, dann ist $\alpha = (e_\alpha) + (e_\beta) + \dots$ eine direkte Summe der Hauptideale (e_λ) , und sie wird ein idempotentes Ideal aus $\mathfrak{R}$.

Wenn $\mathfrak{R} \supset \alpha$ ist, so können wir nach Satz I ein idempotentes Element e_0

ausserhalb von α finden, und das Ideal (e_0) ist idempotent. Dabei können wir nach unserer grundlichen Annahme voraussetzen, dass e_0 ein durch α unteilbares, primitives Element ist. Damit ist offenbar $(e_0) \not\subseteq \alpha$. Setzen wir nun $b = (e_0) \cap \alpha$, so ist $b \subset \alpha$, $b \subset (e_0)$, und ferner nach der Multiplikationseigenschaft von $\mathfrak{R}$ folgt $b = (e_0)b = (e_0)(e_0)b = (e_0)b$, $b = ab' = ab$. Hieraus ergibt sich weiter $b = (e_0)ab \subseteq b^2$, weil $(e_0)\alpha \subseteq b$ ist; also ist b idempotent. Nach Satz I hat b ein idempotentes primitives Element e_0' und $e_0' = e_0 r$ besteht für ein Element r aus $\mathfrak{R}$. Da aber $e_0' e_0 = e_0 r e_0 = r e_0 = e_0' \in b$ ist, so folgt daraus $(e_0 - e_0')e_0' = 0$, $(e_0 - e_0')^2 = e_0 - 2e_0 e_0' + e_0' = e_0 - e_0' \in (e_0)$. Nach der Annahme, dass e_0 ein durch α unteilbares primitives Element ist, soll $e_0' = 0$ und folglich $b = (0)$ sein. Daraus bekommen wir ein Orthogonalsystem von idempotenten, primitiven Elementen, welches grösser als $(e_\alpha, e_\beta, \dots)$ ist. Das widerspricht unserer Annahme, dass $(e_\alpha, e_\beta, \dots)$ maximal ist. Hiermit muss $\mathfrak{R} = \alpha$ sein.

Unsere Aufgabe ist nun die Untersuchung der Struktur eines in direkte Summe unzerlegbaren, idempotenten Multiplikationsringes. Dazu brauchen wir vorerst zu beweisen.

Satz 5. *Ist $\mathfrak{R}$ ein unzerlegbarer, idempotenter Multiplikationsring, so hat $\mathfrak{R}$ Einheits- und sein Radikal ist prim. Hierbei bedeutet Radikal die Gesamtheit aller nilpotenten Elemente von $\mathfrak{R}$.*

Es sei $\mathfrak{h}$ das Radikal von $\mathfrak{R}$, dann ist $\mathfrak{h} \subset \mathfrak{R}$. Denn es gibt in $\mathfrak{R}$ nach Satz I ein idempotentes Element e . Zum Beweise sei $\mathfrak{h}$ nicht prim. Dann besteht $ab \in \mathfrak{h}$ für zwei Elemente a und b mit der Eigenschaft $a \notin \mathfrak{h}$, $b \notin \mathfrak{h}$. Dabei sind beide a und b nicht nilpotent in bezug auf $\mathfrak{h}$, da $\mathfrak{h}$ halbprim ist. Betrachten wir nun $b = \mathfrak{h} : (a)$ und $a = \mathfrak{h} : b$, so wird $b \in b$, $a \in a$. Da $\mathfrak{h}$ halbprim ist, so folgt daraus

$$(1) \quad a \cap b = \mathfrak{h}$$

Aus $a \subset (a, b)$ und nach der Eigenschaft vom Multiplikationsring folgt ferner

$$(2) \quad a = (a, b)c \subseteq c, \quad bc \subseteq a.$$

Nach (1) erhalten wir damit $bc \subseteq \mathfrak{h}$, und folglich besteht $c \subseteq a$. Aus (2) folgt

$$(3) \quad a = c, \quad a = (a, b)a$$

Dabei ist aber $ab \subseteq \mathfrak{h}$, mithin besteht $a = (a^2, \mathfrak{h})$. Nach der Multiplikationseigenschaft ergibt sich $(\mathfrak{h}, a) = ac' = (a^2, \mathfrak{h})c' = (aac' \mathfrak{h}c') = (a(\mathfrak{h}, a), \mathfrak{h}c')$. Daraus erhalten wir

$$(4) \quad a \equiv aa'(\mathfrak{h}), \quad a(a' - a'^3) \equiv 0(\mathfrak{h}),$$

wo a' ein Element aus α ist. Aus (4) und $b = \mathfrak{h} : (\alpha)$ folgt $a' - a'^3 \in b$. Andererseits ist aber $a' - a'^3 \in \alpha$, und folglich erhalten wir nach (1) $a' - a'^3 \in \mathfrak{h}$, und daher auch $(a' - a'^3)^n = 0$ für eine hinreichend grosse natürliche Zahl n . Durch die Entwicklung der Potenz ergibt sich $a'^n = a'^{2n}r$. Setzen wir $a'^n r = e_0$, so ist $e_0 \in \alpha$ und idempotent. Daraus können wir schliessen, dass $\mathfrak{R}$ in direkte Summe zerlegbar, oder $\mathfrak{R} = \alpha$ ist. Der erste Fall widerspricht der im Satz aufgestellten Annahme. Im zweiten Falle ergibt sich $\mathfrak{R}b \subseteq \mathfrak{h}$, $b^2 \subseteq \mathfrak{h}$, im Widerspruch zu $b^2 \notin \mathfrak{h}$. Danach muss das Radikal $\mathfrak{h}$ prim sein.

Nach Satz 1 besitzt $\mathfrak{R}$ ein idempotentes Element e und für ein beliebiges Element r aus $\mathfrak{R}$ gilt $e(r - re) = 0$. Setzen wir m die Gesamtheit aller Elemente m mit der Eigenschaft $em = m$ und n die Gesamtheit aller Elemente n mit der Eigenschaft $en = 0$, so ist $\mathfrak{R}$ in die direkte Summe $\mathfrak{R} = m + n$ zerlegbar. Nach der Unzerlegbarkeit von $\mathfrak{R}$ muss damit $n = (0)$ sein, also $re = r$. Hieraus folgt Satz 5.

Lassen wir uns bei der Weiterentwicklung der Strukturtheorie von Analogieen aus der gewöhnlichen Ringtheorie leiten, so ist das nächste Ziel die Untersuchung von Primidealen. Zunächst wird die Existenz des Primideals durch folgenden Satz hergestellt:

Satz 6. *Wenn $\mathfrak{R}$ ein idempotenter, unzerlegbarer Multiplikationsring ist, so hat jedes Ideal $\alpha (\neq (0), \mathfrak{R})$ einen von $\mathfrak{R}$ verschiedenen Primidealteiler, und die Anzahl der kleinsten Primidealteiler von α ist endlich.*

Zum Beweise sei α ein beliebiges, von Null verschiedenes Ideal aus $\mathfrak{R}$ und $\bar{\mathfrak{R}} = \mathfrak{R}/\alpha$ der Restklassenring von $\mathfrak{R}$ nach α . Dann ist $\bar{\mathfrak{R}}$ auch ein idempotenter Multiplikationsring, und $\bar{\mathfrak{R}}$ hat nach Satz 5 Einheitsselement e . Zu e von $\mathfrak{R}$ ist ein Element $\bar{e}$ von $\bar{\mathfrak{R}}$ zugeordnet, und dabei $\bar{e}$ ist Einheitsselement von $\bar{\mathfrak{R}}$. Nach Satz 4 lässt sich $\bar{\mathfrak{R}}$ als eine direkte Summe $\bar{\mathfrak{R}} = (\bar{e}_1) + (\bar{e}_2) + \dots$ darstellen, wobei $(\bar{e}_1, \bar{e}_2, \dots)$ ein Orthogonalsystem der idempotenten, primitiven Elemente von $\bar{\mathfrak{R}}$ bedeutet. Nach unserer grundsätzlichen Annahme ist aber $\bar{e}$ in eine direkte Summe $\bar{e} = \bar{e}_1' + \bar{e}_2' + \dots + \bar{e}_n'$ von endlich vielen idempotenten, primitiven Elementen $\bar{e}_i'$ zerlegbar, und ferner gehört $\bar{e}_i'$ zu einem aus $(\bar{e}_i)$, weil $\bar{e}_i'$ primitives Element ist. Nach $\bar{e}_i = \bar{e}_i \bar{e} = \bar{e}_i(\bar{e}_1' + \dots + \bar{e}_n')$ besteht damit $\bar{e}_i = \bar{e}_i \bar{e}_i' \in (\bar{e}_i')$, und folglich $(\bar{e}_i) = (\bar{e}_i')$. Daher erkennen wir sofort, dass die Anzahl der Elemente des Orthogonalsystems $(\bar{e}_1, \bar{e}_2, \dots)$ endlich sein muss. Andererseits ist aber nach Satz 5 das Radikal $\bar{\mathfrak{r}}_i$ von $(\bar{e}_i)$ prim, und folglich ist $\bar{\mathfrak{r}}_i + (\bar{e}_1) + \dots + (\bar{e}_{i-1}) + (\bar{e}_{i+1}) + \dots + (\bar{e}_n)$ ein Primideal in $\bar{\mathfrak{R}}$ und ein kleinstes. Damit ist jetzt unsere Behauptung als richtig erkannt.

Aus Satz 6 folgt weiter:

Satz 7. Ist $\mathfrak{R}$ ein idempotenter, unzerlegbarer Multiplikationsring, so ist jedes Primideal $\mathfrak{p} (\neq (0))$ von $\mathfrak{R}$ ein maximales Ideal, und es gibt kein Ideal zwischen $\mathfrak{p}$ und $\mathfrak{p}^2$. Ferner ist jede Potenz von $\mathfrak{p}$ primär und umgekehrt ist ein Primärideal von $\mathfrak{R}$ gleich einer Potenz des zu ihm gehörigen Primideals.

Nach Satz 6 hat $\mathfrak{R}$ einen Primidealteiler $\mathfrak{p} (\neq (0))$, und nach Satz 5 Einheits Elemente e . Aus Satz 1 folgt auch nach Unzerlegbarkeit von $\mathfrak{R}$ $\mathfrak{p}^n \neq \mathfrak{p}^{n-1}$ für jede ganze Zahl n , wenn $\mathfrak{p}$ nicht nilpotent ist.

Wenn $\mathfrak{p}, \mathfrak{m}$ zwei Ideale von der Art sind, dass $\mathfrak{R} \supset \mathfrak{m} \supset \mathfrak{p}$ ist, und wenn $\mathfrak{p}$ prim ist, so gibt es nach der Multiplikationseigenschaft von $\mathfrak{R}$ $\mathfrak{p} = \mathfrak{m}\mathfrak{p}$. Wenn ein Element aus $\mathfrak{p}$ nicht nilpotent ist, so folgt daraus nach Satz 2 die Existenz eines idempotenten Elements in $\mathfrak{m}$ und zwar die Zerlegbarkeit von $\mathfrak{R}$, im Widerspruch zu unserer Annahme. Wenn jedes Element aus $\mathfrak{p}$ nilpotent ist, so ist $\mathfrak{p}$ nach Satz 5 das Radikal von $\mathfrak{R}$. Für ein Element $p (\neq 0)$ aus $\mathfrak{p}$ gilt $(p) = (p)\mathfrak{m}$, und daraus folgt $p = mp$, $p(\mathfrak{m} - \mathfrak{m}^2) = 0$, wobei $m \in \mathfrak{m}$, $m \notin \mathfrak{p}$ ist. Im Falle $m' = \mathfrak{m} - \mathfrak{m}^2 \in \mathfrak{p}$ folgt leicht die Existenz von idempotenten Element im Widerspruch zu der Annahme, dass $\mathfrak{R}$ unzerlegbar ist. Im Falle $m' \notin \mathfrak{p}$ ergibt sich $\mathfrak{p} = (\mathfrak{p}, m')\mathfrak{b}$ und $\mathfrak{b} \subseteq \mathfrak{p}$, weil $m' \notin \mathfrak{p}$ ist. Also erhalten wir $\mathfrak{p} = (\mathfrak{p}, m')\mathfrak{p}$ und daher folgt $(p) = (p)(\mathfrak{p}, m')$. Da $pm' = 0$ ist, so folgt $p = pp_0 = pp_0^2 = 0$, da $p_0 \in \mathfrak{p}$ ist. Das ist aber ein Widerspruch. Zusammenfassend gilt, dass $\mathfrak{p}$ ein maximales Ideal sein soll.

Wäre $\mathfrak{p} \supset \mathfrak{a} \supset \mathfrak{p}^2$, so folgte aus $\mathfrak{a} = \mathfrak{p}\mathfrak{b}$ ein Widerspruch $\mathfrak{a} = \mathfrak{p}$ oder $\mathfrak{a} \subseteq \mathfrak{p}^2$. Denn nach $\mathfrak{b} \supseteq \mathfrak{a} \supset \mathfrak{p}^2$ können wir zwei Fälle betrachten. Im Falle $\mathfrak{b} \subseteq \mathfrak{p}$ ergibt $\mathfrak{a} \subseteq \mathfrak{p}^2$. Im Falle $\mathfrak{b} \not\subseteq \mathfrak{p}$ ist $(\mathfrak{b}, \mathfrak{p}) = \mathfrak{R}$ und daraus folgt $\mathfrak{a} = \mathfrak{p}\mathfrak{b} = \mathfrak{p}(\mathfrak{b}, \mathfrak{p}) = \mathfrak{p}\mathfrak{R} = \mathfrak{p}$, da $\mathfrak{R}$ Einheits element hat. Damit gibt es kein Ideal zwischen $\mathfrak{p}$ und $\mathfrak{p}^2$. Danach erhalten wir

$$(1) \quad \mathfrak{p} = (\pi, \mathfrak{p}^2).$$

Ist $r\mathfrak{p} \equiv 0(\mathfrak{p}^m)$ für zwei Elemente p und r mit der Eigenschaft $p \in \mathfrak{p}$, $p \notin \mathfrak{p}^m$, $r \notin \mathfrak{p}$, so können wir nach (1) $p \equiv r_1\pi + \dots + r_{m-1}\pi^{m-1}(\mathfrak{p}^m)$ setzen, wobei $r_i \notin \mathfrak{p}$ ist, und daraus folgt $rr_1\pi + \dots + rr_{m-1}\pi^{m-1} \equiv 0(\mathfrak{p}^m)$. Da $\mathfrak{p}$ maximal ist, so wird $rr_1r_0 \equiv e(\mathfrak{p})$ für ein Element r_0 . Hieraus folgt $\pi \equiv 0(\mathfrak{p}^2)$, und $\mathfrak{p} = \mathfrak{p}^2$, im Widerspruch zum früher Bewiesenen. Mithin gilt, dass jede Potenz von $\mathfrak{p}$ primär ist.

Endlich sei $\mathfrak{q}$ ein Primärideal und $\mathfrak{h}$ das zu $\mathfrak{q}$ gehörige Halbprimideal, dann ist nach Satz 6 und Primäreigenschaft von $\mathfrak{q}$ $\mathfrak{h}$ ein Primideal. Hiermit setzen wir nun $\mathfrak{h} = \mathfrak{p}$. Wenn $\mathfrak{p}^m \supset \mathfrak{q}$ ist, so wird $\mathfrak{q} = \mathfrak{p}^m\mathfrak{b}_1$ und dabei ist $\mathfrak{b}_1 \subseteq \mathfrak{p}$,

weil q ein zu p gehöriges Primärideal ist. Danach ist $q \subseteq p^{m+1}$. Hieraus folgt also die Aussage: Wenn q gleich keiner Potenz von p ist, so soll q durch jede Potenz von p teilbar sein. Adererseits ist p^m für jede m nicht idempotent und für $b = p \wedge p^2 \wedge p^3 \wedge \dots$ gilt $b = bp \supseteq q$, und folglich $b = b^2$. Denn aus $b = bp \subset p^n$ folgt $b \subset p$, da p^n primär ist. Nach (1) muss damit $b \subseteq p^{n-1}$ sein, was aber für alle n gilt. Also ist $b = 0$. Damit muss nach Satz 1 und der Unzerlegbarkeit von $\mathfrak{R}$ $b = (0)$ sein. Daraus folgt die Behauptung, dass q gleich einer Potenz von p ist.

Jetzt endlich sind wir in der Lage, folgenden Satz zu beweisen.

Satz 8. *Im idempotenten, unzerlegbaren Multiplikationsring $\mathfrak{R}$ lässt sich jedes von Null verschiedene Ideal als ein Produkt von endlich vielen Primidealen eindeutig darstellen. D.h. $\mathfrak{R}$ ist ein Dedekindscher Integritätsbereich, oder ein primärer, einreihiger Ring.*

Zum Beweise sei $a (\neq 0)$ ein beliebiges Ideal von $\mathfrak{R}$ und h das zu a gehörige Halbprimideal. Da wird h nach Sätzen 6 und 7 durch endlich viele Primideale $p_1, p_2, \dots, p_n$ teilbar, und sie sind durch einander unteilbar. Wenn h das Radikal von $\mathfrak{R}$ ist, so wird nach Sätzen 5 und 7 $h = p$ und folglich $a = p^k$.

Im anderen Falle, sei $b = p_1 \wedge p_2 \wedge \dots \wedge p_n$, so wird $b \supseteq h$. Wäre $b \supset h$, so folgte $h = hb \subseteq b$ aus der Multiplikationseigenschaft. Wenn $h = b$ ist, so würde $\mathfrak{R}$ nach Satz 2 in direkte Summe zerlegbar, und im Falle $h \subset b$ wäre $h = b \wedge b$ nach der Eigenschaft von h . Durch Betrachtung von $\mathfrak{R}/h$ ergäbe sich, dass h durch ein von $p_1, p_2, \dots, p_n$ verschiedenes Primideal teilbar wäre. In beiden Fällen hätten wir damit Widerspruch gegen unserer Annahme. Also ist $h = p_1 \wedge p_2 \wedge \dots \wedge p_n$.

Durch Übergang zu den p_i gehörigen isolierten Primärkomponenten q_i von a ergibt sich daraus $a = q_1 \wedge q_2 \wedge \dots \wedge q_n$. Nach Satz 7 ist aber $q_i = p_i^{k_i}$ und $(p_i^{k_i}, p_j^{k_j}) = \mathfrak{R}$ für $i \neq j$. Daraus ergibt sich nämlich sofort: $a = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$ und die Darstellung ist eindeutig.

Nach Satz 5 ist aber das Radikal b von $\mathfrak{R}$ prim, und nach Satz 7 ist b maximal, wenn $b \neq (0)$ ist. Damit gelangen wir zum Schlusse; Im Falle $b = (0)$ ist $\mathfrak{R}$ ein Dedekindscher Integritätsbereich und im anderen Falle $b \neq (0)$ ist $\mathfrak{R}$ ein primärer, einreihiger Ring.

Jetzt können wir die vorig gewonnenen Resultate in dem Hauptsatz dieser Strukturtheorie zusammenfassen:

Satz 9 (Hauptsatz). *Ein idempotenter Multiplikationsring lässt sich als*

eine direkte Summe von endlich oder unendlich vielen Dedekindschen Integritätsbereichen und primären, einreihigen Ringen darstellen.

Zum Schlusse dieses Abschnittes fügen wir noch eine Bemerkung hinzu:

Eine direkte Summe von endlich oder unendlich vielen Dedekindschen Integritätsbereichen und primären, einreihigen Ringen ist umgekehrt ein idempotenter Multiplikationsring.

4. Übersicht.

Um eine Übersicht über die Struktur der Multiplikationsringe und die Relationen zwischen Multiplikationsringe und Z.P.I.-Ringe zu erhalten, fassen wir zunächst die vorig gewonnenen Ergebnisse im Hauptsatz zusammen:

Hauptsatz. *Es sei $\mathfrak{R}$ ein Multiplikationsring und jedes idempotentes Element aus $\mathfrak{R}$ lasse sich als eine direkte Summe von endlich vielen idempotenten, primitiven Elementen darstellen. Im Falle $\mathfrak{R} \neq \mathfrak{R}^2$ ist dann jedes Ideal ($\neq (0)$) aus $\mathfrak{R}$ gleich einer endlichen Potenz von $\mathfrak{R}$, und im Falle $\mathfrak{R} = \mathfrak{R}^2$ ist $\mathfrak{R}$ gleich einer direkten Summe von endlich, oder unendlich vielen Dedekindschen Integritätsbereichen und primären, einreihigen Ringen.*

Nach Krull³⁾ heisst ein kommutativer Ring, in dem jedes Ideal als Produkt von Potenzen endlich vieler Primideale dargestellt werden kann, *allgemeiner Z.P.I.-Ring*. Für diesen Ring ist es schon bewiesen⁴⁾, dass ein kommutativer Ring $\mathfrak{R}$ dann und nur dann ein allgemeiner Z.P.I.-Ring ist, wenn in $\mathfrak{R}$ die folgenden Bedingungen erfüllt sind:

1. *Es gilt in $\mathfrak{R}$ der O-Satz.*
2. *Für jede Primmaximalideale $\mathfrak{p}$ und $\mathfrak{p}'$ existiert kein Zwischenideal zwischen $\mathfrak{p}\mathfrak{p}'$ und $\mathfrak{p}$ (einsch. $\mathfrak{p}=\mathfrak{p}'$).*
3. *Kein Zwischenideal existiert zwischen $\mathfrak{R}$ und $\mathfrak{R}^2$.*

Danach besitzt ein allgemeiner Z.P.I.-Ring die folgende Struktur:

Struktur von allgemeinen Z.P.I.-Ringen.

Im Falle $\mathfrak{R} = \mathfrak{R}^2$ ist $\mathfrak{R} = \mathfrak{R}_1 + \mathfrak{R}_2 + \dots + \mathfrak{R}_n$, wobei $\mathfrak{R}_i$ ein Dedekindscher Integritätsbereich, oder ein primärer einreihiger Ring ist, und im Falle $\mathfrak{R} \neq \mathfrak{R}^2$ ist $\mathfrak{R} = \mathfrak{f} + \mathfrak{m}$, oder $\mathfrak{R} = \mathfrak{m}$, wobei $\mathfrak{f}$ einen Körper und $\mathfrak{m}$ einen Ring bedeutet, in dem jedes Ideal gleich einer Potenz von $\mathfrak{m}$ ist.

Aus dem Hauptsatz und der soeben gesprochenen Tatsache ergibt sich nun der folgende interessante

3) W. Krull, Idealtheorie (1935), 12, 86.

4) S. Mori, Allgemeine Z.P.I.-Ringe, Journal of Sci. of the Hiroshima Univ., Vol. 10 (1940).

Satz 10. *Multiplikationsringe und allgemeine Z.P.I.-Ringe stimmen dann und nur dann miteinander überein, im Falle $\mathfrak{R} = \mathfrak{R}^2$, wenn der Teilerkettensatz gilt, und im Falle $\mathfrak{R} \neq \mathfrak{R}^2$, wenn $\mathfrak{R}$ in direkte Summe unzerlegbar ist. Im Falle $\mathfrak{R} = \mathfrak{R}^2$ ist somit allgemeiner Z.P.I.-Ring nur ein spezieller Fall von Multiplikationsring, in dem der Teilerkettensatz gilt.*

Wir knüpfen endlich noch eine wichtige Bemerkung hier an, dass wir durch eine geringe Verwandlung der Definitionen von Multiplikationsring und Z.P.I.-Ring den Fall $\mathfrak{R} \neq \mathfrak{R}^2$ aus unserer Betrachtung weglassen können.

Z.P.I.-Ring und Multiplikationsring im engeren Sinne. Sind alle Ideale ($\neq \mathfrak{R}$) aus einem Ring $\mathfrak{R}$ als Produkt von endlich vielen Primidealen darstellbar, welche von $\mathfrak{R}$ verschieden sind, so heisst $\mathfrak{R}$ *Z.P.I.-Ring im engeren Sinne*.

Es seien $\mathfrak{a}$ und $\mathfrak{b}$ zwei beliebige Ideale aus Ring $\mathfrak{R}$, und $\mathfrak{a} \subseteq \mathfrak{b}$. Können wir immer ein Ideal $\mathfrak{c}$ von der Art finden, dass $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ ist, so heisst $\mathfrak{R}$ *Multiplikationsring im engeren Sinne*.

Nach den obig ausgesprochenen Eigenschaften von Multiplikationsring und Z.P.I.-Ring im allgemeinen Sinne können wir damit zu folgenden wichtigen Sätzen gelangen:

I. *Jeder Z.P.I.-Ring im engeren Sinne besitzt Einheitsselement und in ihm gilt der Teilerkettensatz.*

Denn, wenn $\mathfrak{R}$ ein Z.P.I.-Ring im engeren Sinne ist, so wird $\mathfrak{R} = \mathfrak{R}^2$ und in $\mathfrak{R}$ gilt der Teilerkettensatz. Daher folgt die Existenz eines Einheitsselements.

II. *Ist $\mathfrak{R}$ ein Multiplikationsring im engeren Sinne, so muss $\mathfrak{R} = \mathfrak{R}^2$ sein.*

III. *Ein Multiplikationsring im engeren Sinne stimmt dann und nur dann mit einem Z.P.I.-Ring im engeren Sinne überein, wenn in ihm der Teilerkettensatz gilt.*