Zusammenhang zwischen Primäridealien und Minimalidealien

Von

Shinziro MORI

(Received Oct. 25, 1930)

In der vorliegenden Abhandlung soll die Untersuchung über die eindeutige Darstellbarkeit des Nullideals als kleinstes gemeinsames Vielfaches von irreduziblen Idealen gegeben werden. Und hierbei wird nur ein kommutativer Ring $\mathfrak{R}$ zugrunde gelegt, der den Doppelketensatz (oder die Existenz einer Hauptkompositionsreihe des Nullideals) erfüllt. Vor kurzer Zeit habe ich den Satz bewiesen⁽¹⁾, dass für jedes Minimalideal $\mathfrak{m}$ der Idealquotient $(0) : \mathfrak{m}$ ein Primideal oder der Ring $\mathfrak{R}$ ist. Hier soll zunächst dieser Satz dazu benutzt werden, um alle Minimalideale in Klassen zu verteilen, und sodann eine Behandlung der Darstellung des Nullideals als Durchschnitt der irreduziblen Ideale oder als Durchschnitt der minimalen Primärideale in Angriff genommen werden.

Unter einem *Minimalideal*⁽²⁾ wird im folgenden ein vom Nullideal verschiedenes Ideal, das nur das Nullideal als echtes Vielfaches hat, verstanden. Ist demnach $\mathfrak{R}$ ein Körper, so wird $\mathfrak{R}$ ein einziges Minimalideal.

§ 1. Klasseneinteilung der Minimalideale

Im folgenden wird der zugrunde gelegte Ring $\mathfrak{R}$ als ein Primideal betrachtet, und Nullprimideal auch angenommen. Nach dem im Anfang ausgesprochenen Satz ist der Idealquotient $(0) : \mathfrak{m}$ damit ein Primideal, wenn $\mathfrak{m}$ ein Minimalideal ist. Demgemäss definieren wir :

Definition : *Ein Minimalideal $\mathfrak{m}$ heisst ein einem Primideal $\mathfrak{p}$ zugeordnetes Minimalideal, wenn der Idealquotient $(0) : \mathfrak{m}$ ein Primideal $\mathfrak{p}$ ist.*

(1) S. Mori, Ueber Primärideale in kommutativen Ringbereichen. *Memoirs of the College of Science, Kyoto Imperial University.*

(2) M. Sono. *On Congruences. Memoirs of the College of Science. Kyoto Imperial University (1917).*

Hiernach leuchtet dann sogleich ein, dass sämtliche Minimalideale des Ringes $\mathfrak{R}$ in Klassen verteilt werden können, von der Art, dass alle Minimalideale derselben Klasse demselben Primideal, zwei Minimalideale verschiedener Klassen aber nicht demselben Primideal entsprechen. Dass die Anzahl dieser Klassen auch endlich ist, ist klar, da die Anzahl der verschiedenen Primideale aus $\mathfrak{R}$ endlich ist. Die genaue Anzahl der Klassen sprechen wir in folgendem Satze aus:

Hilfssatz 1. *Existiert in $\mathfrak{R}$ ein von $\mathfrak{R}$ verschiedenes Primideal, so gibt es in $\mathfrak{R}$ auch ein Minimalideal, das einem von $\mathfrak{R}$ verschiedenen Primideal zugeordnet ist⁽¹⁾.*

Beweis. Wenn $\mathfrak{p}$ ein von $\mathfrak{R}$ verschiedenes Primideal ist, so soll $\mathfrak{R}$ ein nichtnilpotentes Element r enthalten. Es sei die Teilerkette der Idealquotienten gebildet:

$$(0) : \mathfrak{R}r, (0) : \mathfrak{R}r^2, \dots, (0) : \mathfrak{R}r^n, \dots,$$

wobei für jedes n das Ideal $\mathfrak{R}r^n$ vom Nullideal verschieden ist. Dann bricht nach dem Doppelkettensatz die Kette im Endlichen ab, und wir erhalten:

$$(0) : \mathfrak{R}r^n = (0) : \mathfrak{R}r^{n+1} = (0) : \mathfrak{R}r^{n+2} \quad (1)$$

für eine endliche Zahl n . Ferner soll $\mathfrak{R}r^{n+1}$ ein Minimalideal $\mathfrak{m}$ enthalten und der Idealquotient $(0) : \mathfrak{m}$ auch ein Primideal sein. Wenn $\mathfrak{R} = (0) : \mathfrak{m}$ wäre, so würde $\mathfrak{R}\mathfrak{m} = (0)$. Da $\mathfrak{m}$ durch $\mathfrak{R}r^{n+1}$ teilbar ist, so hätten wir

$$r' r^{n+1} \neq 0, \quad r' r^{n+2} = 0,$$

wo r' ein Element aus $\mathfrak{R}$ ist. Also würden

$$r' \neq 0 \quad ((0) : \mathfrak{R}r^n), \quad r' \equiv 0 \quad ((0) : \mathfrak{R}r^{n+2})$$

im Widerspruch mit (1). Hiermit ist $(0) : \mathfrak{m}$ ein von $\mathfrak{R}$ verschiedenes Primideal.

Hilfssatz 2. *Es werden alle Minimalideale in Klassen verteilt und seien $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_m$ alle verschiedenen zugeordneten Primideale, die sämtlich von $\mathfrak{R}$ verschieden sind. Dann ist $\mathfrak{d} = [\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_m]$ ein nilpotentes Ideal.*

(1) Existiert in $\mathfrak{R}$ kein von $\mathfrak{R}$ verschiedenes Primideal ($\neq 0$), so ist $\mathfrak{R}$ ein nilpotenter Ring oder ein Körper. Denn, wenn es in $\mathfrak{R}$ ein nichtnilpotentes Element gibt, so existiert in $\mathfrak{R}$ auch ein idempotentes Element e . Ein nicht e enthaltendes Maximalideal ist offenbar ein Primideal (§ 3) und folglich enthalten alle Ideale ($\neq 0$) das Element e ; also ist $\mathfrak{R}$ ein Körper, der e als Einheitselement enthält.

Beweis. Wenn δ nicht nilpotent ist, so gibt es in δ ein nichtnilpotentes Element d . Für die Teilerkette der Idealquotienten

$$(0) : \mathfrak{R}d, \quad (0) : \mathfrak{R}d^2, \quad \dots, \quad (0) : \mathfrak{R}d^n, \quad \dots$$

ergibt sich daher

$$(0) : \mathfrak{R}d^n = (0) : \mathfrak{R}d^{n+1} = (0) : \mathfrak{R}d^{n+2}.$$

Sei nun m ein Minimalideal, das durch $\mathfrak{R}d^{n+1}$ teilbar ist, dann wird nach dem Beweis des Hilfssatzes 1 m ein einem von $\mathfrak{R}$ verschiedenen Primideal $\mathfrak{p}$ zugeordnetes Minimalideal und $\mathfrak{p}$ soll identisch mit irgendwelchem von $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_m$ sein. Damit folgen wegen $\mathfrak{p}m=0$

$$rd^{n+2}=0, \quad rd^{n+1} \neq 0,$$

wobei r ein Element aus $\mathfrak{R}$ ist, da δ durch $\mathfrak{p}$ teilbar ist.

Also erhalten wir

$$r \equiv 0 \pmod{(0) : \mathfrak{R}d^{n+2}}, \quad r \not\equiv 0 \pmod{(0) : \mathfrak{R}d^n},$$

damit ist ein Widerspruch nachgewiesen. Mithin sind alle Elemente aus δ nilpotent, δ muss also auch nilpotent sein.

Hieraus ergibt sich nun

Satz 1. Wenn $\mathfrak{p}$ ein von $\mathfrak{R}$ verschiedenes Primideal ist, so gibt es in $\mathfrak{R}$ auch ein $\mathfrak{p}$ zugeordnetes Minimalideal.

Es seien $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_m$ alle von $\mathfrak{R}$ verschiedenen Primideale, für die die zugeordneten Minimalideale existieren. Dann kommt nach Hilfssatz 2:

$$(\mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_m)^\rho = (0), \quad \text{für eine endliche Zahl } \rho.$$

Wenn das gegebene Primideal $\mathfrak{p}$ von jedem aus $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_m$ verschieden wäre, hätten wir daher

$$(\mathfrak{p}_1 \mathfrak{p}_2, \dots, \mathfrak{p}_m)^\rho \equiv 0 \pmod{\mathfrak{p}},$$

wo $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_m$ die Elemente aus $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ ausserhalb $\mathfrak{p}$ sind. Das widerspricht der Tatsache, dass $\mathfrak{p}$ ein Primideal ist. Damit muss in $\mathfrak{R}$ ein einem beliebigen Primideal ($\neq \mathfrak{R}$) zugeordnetes Minimalideal existieren.

Zusatz. Die Anzahl der Minimalidealklassen ist gleich der Anzahl der von $\mathfrak{R}$ verschiedenen Primideale oder der Anzahl aller Primideale, jenachdem, ob $\mathfrak{R}$ Einheitsselement enthält oder nicht.

Wenn $\mathfrak{R}$ Einheitsselement enthält, so gilt es kein $\mathfrak{R}$ zugeordnetes Minimalideal. Enthält $\mathfrak{R}$ dagegen kein Einheitsselement, so gibt es in $\mathfrak{R}$ einen Totalnullteiler⁽¹⁾ ausser Null; also existiert ein $\mathfrak{R}$ zugeordnetes Minimalideal. Ferner ist nach Satz 1 die Anzahl der Minimalidealklassen, die den von $\mathfrak{R}$ verschiedenen Primidealen zugeordnet sind, gleich der Anzahl der Primideale ($\neq \mathfrak{R}$); woraus der Zusatz folgt.

Wenn $\mathfrak{m}$ ein Minimalideal ist, so gilt

$$\mathfrak{m}^2 = \mathfrak{m} \quad \text{oder} \quad \mathfrak{m}^2 = (0).^{(2)}$$

Im ersten Falle heisst $\mathfrak{m}$ ein *idempotentes Minimalideal* und anderenfalls heisst $\mathfrak{m}$ ein *nilpotentes Minimalideal*.

Nach der Unterscheidung der Minimalideale gilt es

Satz 2. *Wenn ein idempotentes Minimalideal $\mathfrak{m}$ zu einer Minimalidealklasse gehört, so gibt es in der Klasse kein Minimalideal ausser $\mathfrak{m}$.*

Ein $\mathfrak{m}$ zugeordnetes Primideal $\mathfrak{p}$ ist von $\mathfrak{R}$ verschieden und $\mathfrak{m} \not\equiv 0 \pmod{\mathfrak{p}}$, da $\mathfrak{m}$ idempotent ist. In unserem Ring wird jedes Primideal zugleich ein Maximalideal, somit erhalten wir

$$\mathfrak{R} = (\mathfrak{p}, \mathfrak{m}).$$

Sei nun $\mathfrak{m}'$ ein von $\mathfrak{m}$ verschiedenes Minimalideal, das auch $\mathfrak{p}$ entspricht. Dann werden

$$\mathfrak{p}\mathfrak{m}' = (0), \quad \mathfrak{m}\mathfrak{m}' = (0).$$

Hieraus folgt

$$\mathfrak{m}'(\mathfrak{p}, \mathfrak{m}) = \mathfrak{m}'\mathfrak{R} = (0);$$

was einen Widerspruch darstellt.

Zusatz. *Es sein $\mathfrak{m}_1, \mathfrak{m}_2, \dots, \mathfrak{m}_i, \dots, \mathfrak{m}_n$ die n verschiedenen idempotenten Minimalideale und $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ die zugeordneten Primideale. Dann ist $\mathfrak{R}$ als direkte Summe⁽³⁾ von der Form*

$$\mathfrak{R} = \mathfrak{m}_1 + \mathfrak{m}_2 + \dots + \mathfrak{m}_n + \mathfrak{d}$$

(1) S. Mori, Ueber Primärdeale in kommutativen Ringbereichen.

(2) M. Sono, On Congruences.

(3) Für den Begriff der direkten Summe vgl. E. Noether, Abstrakter Aufbau der Idealtheorie, Math. Ann. 96.

darstellbar, wobei $\delta = [p_1, p_2, \dots, p_n]$ ist.

Beweis. Jedes der Minimalideale $m_1, \dots, m_n$ ist nicht durch den grössten gemeinsamen Teiler der anderen Minimalideale teilbar. Denn, wenn etwa $m_1 \equiv 0 \pmod{(m_2, \dots, m_n)}$ wäre, so würde durch Multiplikation mit m_1

$$m_1^2 = (0),$$

was unmöglich ist. Also wird

$$(m_1, m_2, \dots, m_n) = m_1 + m_2 + \dots + m_n.$$

Da die idempotenten Minimalideale nicht durch die zugeordneten Primideale teilbar sind, so ist jedes aus $m_1, \dots, m_n$ auch nicht durch δ teilbar. Damit wird $[m_1 + \dots + m_n, \delta] = (0)$, denn es gibt ein Element p_j derart, dass

$$m_j p_j = m_j, \quad m_i p_j = (0) \quad (i \neq j).$$

Andererseits erhalten wir

$$\mathfrak{R} = (m_i, p_i) \quad (i=1, 2, \dots, n),$$

daraus folgt für jedes Element r aus $\mathfrak{R}$

$$r = m_1 + p_1 = m_2 + p_2 = \dots = m_n + p_n$$

wo m_i Elemente aus m_i und p_i Elemente aus p_i sind. Mithin

$$\begin{aligned} r - (m_1 + \dots + m_n) &= p_1 - (m_2 + \dots + m_n) = \dots \\ &= p_n - (m_1 + m_2 + \dots + m_{n-1}). \end{aligned}$$

Seien nun $i \neq j$ $1 \leq i, j \leq n$, dann werden $m_j \equiv 0 \pmod{(p_i)}$, da sonst $m_i m_j = (0)$ einen Widerspruch gegen Primideal p_i darstellen. Hieraus folgen

$$r - (m_1 + \dots + m_n) \equiv 0 \pmod{(p_i)} \quad (i=1, 2, \dots, n),$$

oder

$$r - (m_1 + m_2 + \dots + m_n) \equiv 0 \pmod{\delta}.$$

Damit erhalten wir

$$\mathfrak{R} = m_1 + m_2 + \dots + m_n + \delta.$$

§ 2. Unabhängige Minimalideale

Definition. Ist keines der Minimalideale $m_1, m_2, \dots, m_n$ durch den grössten gemeinsamen Teiler der anderen Minimalideale teilbar, so nennen wir die Minimalideale, „unabhängig voneinander.“

Die idempotenten Minimalideale sind unabhängig voneinander und die ihnen entsprechenden Klassen bestehen aus einem Minimalideal. Wir beschäftigen uns damit im folgenden mit den Eigenschaften des grössten gemeinsamen Teilers aller nilpotenten Minimalideale, welche zu derselben Klasse gehören. $\mathfrak{M}_i$ ($i=0, 1, \dots, m$) werden als grösste gemeinsame Teiler aller Minimalideale, die p_i zugeordnet sind, bezeichnet, insbesondere bedeutet $\mathfrak{M}_0$ den gr. gem. Teiler, der $\mathfrak{R}=p_0$ zugeordnet ist.

Wenn ein $\mathfrak{R}$ zugeordnetes Minimalideal existiert, so ist das Ideal $\mathfrak{M}_0$ bei Komposition durch Addition zugleich eine endliche Abelsche Gruppe und umgekehrt ist jede Untergruppe von $\mathfrak{M}_0$ zugleich ein Ideal aus $\mathfrak{R}$, da der Doppelkettensatz erfüllt ist und alle Elemente aus $\mathfrak{M}_0$ Totalnullteiler sind. Damit gibt es in $\mathfrak{M}_0$ eine Basis $M_1, M_2, \dots, M_{n_0}$ ⁽¹⁾ und in unserem Falle ist der Grad jedes Basiselement M_i eine Primzahl p_i . Damit werden die Minimalideale (M_i) unabhängig voneinander und $\mathfrak{M}_0$ ist in der Form

$$\mathfrak{M}_0 = (M_1) + (M_2) + \dots + (M_{n_0})$$

darstellbar.⁽²⁾

Satz 3. Die Darstellung von $\mathfrak{M}_0$ als direkte Summe der Minimalideale ist dann und nur dann eindeutig bestimmt, wenn $\mathfrak{M}_0$ zyklisch ist.

Beweis. Wenn $\mathfrak{M}_0$ zyklisch ist, so soll die zu einer Primzahl p gehörige Basiszahl gleich 1 sein. Damit sind in der Darstellung

$$\mathfrak{M}_0 = (M_1) + \dots + (M_{n_0}) \quad (1)$$

alle Minimalideale eindeutig bestimmt. Also ist die Bedingung hinreichend.

Die Bedingung ist aber auch notwendig. Denn, wenn etwa die Grade von M_1 und M_2 in der Darstellung (1) gleich einer Primzahl p_1 wären, so wäre die Darstellung

(1) A. Speiser, Theorie der Gruppen von endlicher Ordnung. § 15.

E. Hecke, Theorie der algebraischen Zahlen § 8.

(2) Sei $t=(0): \mathfrak{R}$. Dann bildet die Gesamtheit aller Elemente aus t , deren Grad eine Primzahl oder eine Zahl von der Form $p_1 p_2 \dots p_l$ ist, ein Ideal. Das Ideal ist identisch mit $\mathfrak{M}_0$. t ist dann und nur dann zyklisch, wenn $\mathfrak{M}_0$ zyklisch ist.

$$\mathfrak{M}_0 = (M_1 - M_2) + (M_2) + (M_3) + \dots + (M_{n_0})$$

auch eine direkte Summe von Minimalidealien und von der Darstellung (1) verschieden, da $M_1, M_2, \dots, M_{n_0}$ eine Basis von $\mathfrak{M}_0$ sind. Damit muss die zu p_i gehörige Basiszahl gleich 1 sein; also soll $\mathfrak{M}_0$ eine zyklische Abelsche Gruppe sein.

Und nun beweisen wir folgenden Satz, der uns völligen Aufschluss über die Struktur der grössten gemeinsamen Teiler $\mathfrak{M}_i$ gibt, die den von $\mathfrak{R}$ verschiedenen Primidealien p_i entsprechen.

Satz 4. $\mathfrak{M}_i$ sind auch als direkte Summe von endlich vielen Minimalidealien, die p_i ($i \neq 0$) zugeordnet sind, darstellbar und die Anzahl der Minimalideale in der Darstellung ist eindeutig bestimmt.

Beweis. Wir betrachten nun den gr. gem. Teiler von zwei verschiedenen Minimalidealien m_{i1}, m_{i2} , die p_i zugeordnet sind. Wenn $\mathfrak{M}_i = (m_{i1}, m_{i2})$ ist, so wird auch

$$\mathfrak{M}_i = m_{i1} + m_{i2} .$$

Im anderen Falle sei m_{i3} ein p_i zugeordnetes Minimalideal ausserhalb von (m_{i1}, m_{i2}) und es sei (m_{i1}, m_{i2}, m_{i3}) auch gebildet. In dieser Weise müssen wir endlich die Beziehung

$$\mathfrak{M}_i = (m_{i1}, m_{i2}, \dots, m_{in_i})$$

erhalten, da der Doppelkettensatz erfüllt ist.

Ferner sind $m_{i1}, \dots, m_{in_i}$ unabhängig von einander. Denn, wenn

$$m_{ij} \equiv 0 \quad ((m_{i1}, \dots, m_{ij-1}, m_{ij+1}, \dots, m_{in_i}))$$

wäre, so würde

$$m_{ij} = m_{i1} + \dots + m_{ij-1} + m_{ij+1} + \dots + m_{in_i} ,$$

oder

$$m_{in_i} = m_{ij} - (m_{i1} + \dots + m_{in_i-1}) ,$$

wobei $m_{i1}, \dots, m_{in_i}$ die Elemente aus $m_{i1}, m_{i2}, \dots, m_{in_i}$ sind; also wäre m_{in_i} in $(m_{i1}, \dots, m_{in_i-1})$ enthalten. Das widerspricht der Tatsache, dass m_{in_i} ausserhalb von $(m_{i1}, \dots, m_{in_i-1})$ liegt.

Damit wird

$$\mathfrak{M}_i = m_{i1} + m_{i2} + \dots + m_{in_i} .$$

Es seien zwei Darstellungen

$$\mathfrak{M}_i = m_{i1} + m_{i2} + \dots + m_{in_i}, \quad \mathfrak{M}_i = m'_{i1} + m'_{i2} + \dots + m'_{in'_i}$$

vorgelegt, wobei alle Minimalideale $\mathfrak{p}_i$ zugeordnet sind. Wenn $n_i > n'_i$ ist, erhalten wir die Beziehungen

$$\begin{aligned} m_{i1} &= x_{11}m'_{i1} + x_{12}m'_{i2} + \dots + x_{1n'_i}m'_{in'_i} \\ m_{i2} &= x_{21}m'_{i1} + x_{22}m'_{i2} + \dots + x_{2n'_i}m'_{in'_i} \\ &\dots \dots \dots \\ m_{in'_i} &= x_{n'_i1}m'_{i1} + x_{n'_i2}m'_{i2} + \dots + x_{n'_in'_i}m'_{in'_i} \\ m_{in'_i+1} &= x_{n'_i+11}m'_{i1} + x_{n'_i+12}m'_{i2} + \dots + x_{n'_i+1n'_i}m'_{in'_i}, \end{aligned}$$

wo $m_{i1}, \dots, m_{in'_i+1}$ die von Null verschiedenen Elemente aus $m_{i1}, \dots, m_{in'_i+1}$, $m'_{i1}, \dots, m'_{in'_i}$ die Elemente aus $m'_{i1}, \dots, m'_{in'_i}$ und die Koeffizienten $x_{11}, x_{12}, \dots, x_{n'_i+1n'_i}$ die Elemente aus $\mathfrak{R}$ sind, da $m'_{ij} = \mathfrak{R} m'_{ij}$ sind. Dazu sollen die Koeffizienten nicht durchweg durch $\mathfrak{p}_i$ teilbar sein. Seien nun $A_j^{(i)}$ die Komplemente der Elemente m_{ij} aus der Determinante

$$\begin{vmatrix} m_{i1} & x_{11} & \cdot & \cdot & x_{1n'_i} \\ m_{i2} & x_{21} & \cdot & \cdot & x_{2n'_i} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ m_{in'_i} & x_{n'_i1} & \cdot & \cdot & x_{n'_in'_i} \\ m_{in'_i+1} & x_{n'_i+11} & \cdot & \cdot & x_{n'_i+1n'_i} \end{vmatrix}$$

Dann erhalten wir $A_1^{(i)}m_{i1} + \dots + A_{n'_i+1}^{(i)}m_{in'_i+1} = 0$. Da $m_{i1}, \dots, m_{in'_i}$ aber unabhängig voneinander sind, so müssen

$$A_j^{(i)} \equiv 0 \pmod{\mathfrak{p}_i} \quad (j=1, 2, \dots, n'_i+1)$$

sein. Weiter seien $A_{jk}^{(i)}$ die Komplemente der Elemente x_{jk} aus der Determinante

$$\Delta = \begin{vmatrix} x_{11} & x_{12} & \cdot & \cdot & x_{1n'_i} \\ x_{21} & x_{22} & \cdot & \cdot & x_{2n'_i} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ x_{n'_i1} & x_{n'_i2} & \cdot & \cdot & x_{n'_i n'_i} \end{vmatrix} \equiv 0 \pmod{p_i}$$

Dann werden wegen

$$A_{1k}^{(i)} m_{i1} + A_{2k}^{(i)} m_{i2} + \dots + A_{n'_i k}^{(i)} m_{in'_i} = 0 \quad (k=1, 2, \dots, n'_i)$$

auch

$$A_{jk}^{(i)} \equiv 0 \pmod{p_i} \quad (j, k=1, 2, \dots, n'_i)$$

da $p_i \mid m'_{ij} = (0)$ sind. Also ist der Rang von Δ in bezug auf p_i niedriger als $n'_i - 1$.

Durch wiederholte Anwendung dieses Verfahrens ergibt sich aber endlich $x_{jk} \equiv 0 \pmod{p_i}$ ($j, k=1, 2, \dots, n'_i$) im Widerspruch. Hiermit muss $n_i = n'_i$ sein, also ist der Satz in allen seinen Teilen bewiesen.

Zusatz.

$$[\mathfrak{M}_i, \mathfrak{M}_j] = (0) \quad \text{für } i \neq j, \quad 0 \leq i, j \leq m,$$

wo m die Anzahl der von $\mathfrak{R}$ verschiedenen Primideale ist.

Zusatz. Ist $\mathfrak{M}_i$ ($i \neq 0$) als direkte Summe der Minimalideale darstellbar, so gilt die Eindeutigkeit der Darstellung nicht mehr.

Es sei nun

$$\mathfrak{M}_i = \mathfrak{m}_{i1} + \mathfrak{m}_{i2} + \dots + \mathfrak{m}_{in_i} = \mathfrak{R}m_{i1} + \mathfrak{R}m_{i2} + \dots + \mathfrak{R}m_{in_i},$$

wo m_{ij} die Elemente aus $\mathfrak{m}_{ij}$ sein. Da der Restklassenring $\mathfrak{R}/p_i$ ein Körper ist, so wird $\mathfrak{R}(m_{i1} - m_{i2})$ auch ein von $\mathfrak{R}m_{i1}$ verschiedenes Minimalideal und dazu sind $\mathfrak{R}(m_{i1} - m_{i2}), \mathfrak{R}m_{i2}, \dots, \mathfrak{R}m_{in_i}$ auch unabhängig voneinander; woraus

$$\mathfrak{M}_i = \mathfrak{R}(m_{i1} - m_{i2}) + \mathfrak{R}m_{i2} + \dots + \mathfrak{R}m_{in_i}.$$

Bei idempotenten Minimalidealen $\mathfrak{m}_i$ sind auch $\mathfrak{M}_i = \mathfrak{m}_i$; also ergibt sich nach Satz 4 unmittelbar.

Satz 5. Der grösste gemeinsame Teiler $\mathfrak{M}$ aller Minimalideale aus $\mathfrak{R}$ ist auch als direkte Summe von n Minimalidealen darstellbar, und die Anzahl n ist unabhängig von der Auswahl der unabhängigen Minimalideale.

Satz 6. Wenn für ein Ideal α $\mathfrak{p}\alpha=(0)$, $\mathfrak{p}$ ein Primideal ist, dann wird

$$\alpha = \mathfrak{m}_1 + \dots + \mathfrak{m}_l + \mathfrak{m},$$

wobei $\mathfrak{m}_i$ die $\mathfrak{p}$ zugeordneten Minimalideale sind und $\mathfrak{R}\mathfrak{m}=(0)$ ist.

Beweis. Die Gesamtheit aller Elemente m aus α von der Eigenschaft, dass $\mathfrak{R}m=(0)$ ist, bildet ein Ideal $\mathfrak{m}$. Existiert ein Element a_1 in α ausserhalb von $\mathfrak{m}$, so wird $\mathfrak{R}a_1=\mathfrak{m}_1$ ein Minimalideal. Denn, da der Restklassenring $\mathfrak{R}/\mathfrak{p}$ ein Körper ist, gibt es für beliebige Elemente r_1, r_2 aus $\mathfrak{R}$ ausserhalb von $\mathfrak{p}$ ein Element r_3 derart, dass $r_1 \equiv r_2 r_3 \pmod{\mathfrak{p}}$ ist. Und dazu ist auch

$$[\mathfrak{m}_1, \mathfrak{m}] = (0).$$

Wenn $\alpha = \mathfrak{m}_1 + \mathfrak{m}$ ist, so ist der Satz schon bewiesen. Im anderen Falle sei a_2 ein Element aus α ausserhalb von $\mathfrak{m}_1 + \mathfrak{m}$, dann wird $\mathfrak{R}a_2 = \mathfrak{m}_2$ auch ein Minimalideal und

$$[\mathfrak{m}_2, \mathfrak{m}_1 + \mathfrak{m}] = (0).$$

Sonst würde $\mathfrak{m}_2 \equiv 0 \pmod{\mathfrak{m}_1 + \mathfrak{m}}$, $r_2 a_2 = r_1 a_1 + m$;
also würden

$$r_2 r_3 a_2 = r_1 a_2 = r_1 r_3 a_1, \quad r_1(a_2 - r_3 a_1) = 0, \quad \mathfrak{R}(a_2 - r_3 a_1) = (0).$$

Damit würde

$$a_2 - r_3 a_1 \equiv 0 \pmod{\mathfrak{m}}, \quad \text{oder} \quad a_2 \equiv 0 \pmod{\mathfrak{m}_1 + \mathfrak{m}}$$

mit Widerspruch. Daraus ist es auch klar, dass $\mathfrak{m}_1, \mathfrak{m}_2, \mathfrak{m}$ unabhängig voneinander sind. Indem wir so fortfahren, bis alle Elemente aus α erschöpft sind, erhalten wir endlich

$$\alpha = \mathfrak{m}_1 + \mathfrak{m}_2 + \dots + \mathfrak{m}_l + \mathfrak{m}$$

Satz 7. Sei $(0) = [r_1, r_2, \dots, r_n]$ eine kürzeste Darstellung des Nullideals als kleinstes gemeinsames Vielfaches von irreduziblen. Dann ist die Anzahl der Komponenten gleich der Anzahl der unabhängigen Minimalideale derart, dass jedes Minimalideal aus $\mathfrak{R}$ durch ihre direkte Summe teilbar ist.

Beweis. Seien nun

$$\mathfrak{d}_i = [r_1, \dots, r_{i-1}, r_{i+1}, \dots, r_n] \quad (i=1, 2, \dots, n).$$

Dann werden

$$[r_i, \delta_i] = (0), \quad \delta_i \neq (0).$$

Es seien auch m_i die durch δ_i teilbaren Minimalideale, dann sind m_i unabhängig voneinander, da

$$m_i \neq 0 (r_i), \quad m_j \equiv 0 (r_i) \quad i \neq j.$$

Sind m'_i die nicht durch r_i teilbaren Minimalideale, so müssen

$$[(r_i, m_i), (r_i, m'_i)] \supset r_i$$

sein, da r_i irreduzibel sind. Daraus folgen

$$m'_i \equiv 0 ((r_i, m_i));$$

also geben es in δ_i nur ein einziges Minimalideal m_i , da $[r_i, \delta_i] = (0)$ sind.

Sei nun m auch ein beliebiges Minimalideal und sei durch $r_1, r_2, \dots, r_j$, aber nicht durch $r_{j+1}, \dots, r_n$ teilbar. Dann werden

$$m = m_{j+1} + r_{j+1} = m_{j+2} + r_{j+2} = \dots = m_n + r_n,$$

wobei $m, m_{j+1}, \dots, m_n$ die Elemente von $m, m_{j+1}, \dots, m_n$ und $r_{j+1}, \dots, r_n$ die Elemente aus $r_{j+1}, \dots, r_n$ sind. Hieraus folgt

$$-m_{j+1} + r_{j+2} = -m_{j+2} + r_{j+1} = C_{j+1, j+2},$$

wo $C_{j+1, j+2}$ durch r_{j+1}, r_{j+2} teilbar ist; also erhalten wir

$$m = m_{j+1} + m_{j+2} + C_{j+1, j+2} = m_{j+3} + r_{j+3} = \dots = m_n + r_n.$$

Daraus folgt wieder

$$-(m_{j+1} + m_{j+2}) + r_{j+3} = -m_{j+3} + C_{j+1, j+2} = C_{j+1, j+2, j+3},$$

wo $C_{j+1, j+2, j+3}$ durch $r_{j+1}, r_{j+2}, r_{j+3}$ teilbar ist; also erhalten wir auch

$$m = m_{j+1} + m_{j+2} + m_{j+3} + C_{j+1, j+2, j+3} = \dots = m_n + r_n.$$

Indem wir so fortfahren, erhalten wir schliesslich

$$m = m_{j+1} + m_{j+2} + \dots + m_n + C_{j+1, \dots, n},$$

wo $C_{j+1, j+2, \dots, n}$ durch $r_{j+1}, r_{j+2}, \dots, r_n$ teilbar ist. In der Formel

$$m - (m_{j+1} + \dots + m_n) = C_{j+1, j+2, \dots, n}$$

ist das Element linker Hand durch $r_1, r_2, \dots, r_j$ teilbar und das Element rechter Hand ist durch $r_{j+1}, r_{j+2}, \dots, r_n$ teilbar. Da $(0)=[r_1, r_2, \dots, r_n]$ aber ist, so muss

$$m - (m_{j+1} + \dots + m_n) = C_{j+1 j+2 \dots n} = 0$$

sein.

Hiermit sind alle Minimalideale durch $m_1 + m_2 + \dots + m_n$ teilbar, also ist der Satz bewiesen.

Aus den Sätzen 5,7 folgt weiter :

Zusatz: Die Anzahl der Komponenten in der kürzesten Darstellung des Nullideals als kleinstes gemeinsames Vielfaches von irreduziblen Idealen ist eindeutig bestimmt⁽¹⁾.

§ 3. Die zu m elementfremden Maximalideale

Sind $m_1, m_2, \dots, m_n$ die voneinander unabhängigen Minimalideale, so existiert auch nach dem Doppelkettensatz ein Ideal g_i von der Art, dass $[m_i, g_i] = (0)$ und jeder echte Teiler von g_i ein von Null verschiedenes gemeinsames Element mit m_i enthält. Auf Grund dieser Betrachtung wollen wir die folgende Definition aufstellen.

Definition. Gilt die Beziehung $[\alpha, g] = (0)$ für die Ideale α und g , aber keine Beziehung $[\alpha, g'] = (0)$ für jeden echten Teiler g' von g , so heisst g ein zu α elementfremdes Maximalideal.

Daraus folgt unmittelbar

Ist m ein Minimalideal und ist g ein zu m elementfremdes Maximalideal, so wird g irreduzibel,

Wenn g reduzibel wäre, so gäben es zwei echte Teiler g_1, g_2 von g . Das ist aber nicht möglich, da nach der Voraussetzung g_1 und g_2 das Minimalideal m enthalten müssen.

Satz 8. Ist g ein zu einem Minimalideal m elementfremdes Maximalideal und ist p das m zugeordnete Primideal, so wird g ein zu p gehöriges Primärideal.

Beweis. Da $p = (0) : m$ und $[m, g] = (0)$ ist, so wird

$$g \equiv 0 \pmod{p}.$$

Ist $p^n \not\equiv 0 \pmod{g}$ für jedes n , so können wir in p ein Element p finden, sodass für jedes n $p^n \equiv 0 \pmod{g}$ ist. Damit ist das Ideal $\mathcal{R}p^n$ für jedes n

(1) Der Satz unter Voraussetzung des Teilerkettensatzes findet sich schon bei E. Noether, Idealtheorie in Ringbereichen. Math. Ann. 83.

stets nicht durch $\mathfrak{g}$ teilbar. Nach der Voraussetzung können wir in der Teilerkette der Idealquotienten

$$\mathfrak{g} : \mathfrak{R}p, \mathfrak{g} : \mathfrak{R}p^2, \dots, \mathfrak{g} : \mathfrak{R}p^s, \dots$$

die Beziehung

$$\mathfrak{g} : \mathfrak{R}p^s = \mathfrak{g} : \mathfrak{R}p^{s+1} = \mathfrak{g} : \mathfrak{R}p^{s+2} \quad (1)$$

finden. Setzen wir nun $(\mathfrak{g}, \mathfrak{R}p^{s+1}) = \mathfrak{g}'$, dann wird

$$m \equiv 0 (\mathfrak{g}'),$$

da $\mathfrak{g}'$ ein echter Teiler von $\mathfrak{g}$ ist. Für ein Element m aus $\mathfrak{m}$ erhalten wir also

$$m = g + rp^{s+1}, \quad rp^{s+1} \not\equiv 0 (\mathfrak{g}),$$

wo g ein Element aus $\mathfrak{g}$ und r ein Element aus $\mathfrak{R}$ ist. Wegen $m\mathfrak{p} = (0)$ folgen durch Multiplikation mit p

$$rp^{s+2} \equiv 0 (\mathfrak{g}), \quad rp^{s+1} \not\equiv 0 (\mathfrak{g}),$$

Daraus folgen auch

$$r \equiv 0 (\mathfrak{g} : \mathfrak{R}p^{s+2}), \quad r \not\equiv 0 (\mathfrak{g} : \mathfrak{R}p^s),$$

mit Widerspruch gegen (1). Hiermit wird

$$\mathfrak{p}^n \equiv 0 (\mathfrak{g}), \quad \text{für eine endliche Zahl } n.$$

Wenn $\mathfrak{p} = \mathfrak{R}$ ist, so ist es klar, dass $\mathfrak{g}$ ein zu $\mathfrak{R}$ gehöriges Primärideal ist. Im anderen Falle nehmen wir ein Element r' ausserhalb von $\mathfrak{p}$ und ein Element p' in $\mathfrak{p}$ ausserhalb $\mathfrak{g}$. Dann wird stets

$$r'p' \not\equiv 0 (\mathfrak{g}).$$

Sonst würde $m'r' \equiv 0 (\mathfrak{g})$, wobei $m' (\neq 0)$ ein Element aus $\mathfrak{m}$ ist; also würde

$$m'r' = 0,$$

da $[\mathfrak{m}, \mathfrak{g}] = (0)$ ist. Damit wäre wegen $m'\mathfrak{p} = (0)$

$$m'\mathfrak{R} = (0), \quad \text{oder} \quad \mathfrak{m}\mathfrak{R} = (0)$$

mit Widerspruch.

Hiermit ist der Satz bewiesen.

Nach der Voraussetzung des Doppelkettensatzes erkennen wir sofort, dass der Ring $\mathfrak{R}$ nur endlich viele verschiedene minimale Primär ideale enthält. Daraus ergibt sich leicht

Zusatz 1. Sind $q_1, q_2, \dots, q_m, q_0$ alle verschiedenen minimalen Primär ideale und gehört q_0 zu $\mathfrak{R}$, so wird

$$(0) = [q_1, q_2, \dots, q_m, q_0], \text{ wenn } \mathfrak{R}^2 \neq \mathfrak{R},$$

$$(0) = [q_1, q_2, \dots, q_m], \text{ wenn } \mathfrak{R}^2 = \mathfrak{R}$$

und die Darstellung ist auch die kürzeste.

Wenn $\mathfrak{d} = [q_1, q_2, \dots, q_m, q_0] \neq (0)$ ist, können wir ein Minimalideal $\mathfrak{m}$, das durch $\mathfrak{d}$ teilbar ist, finden. Sei $\mathfrak{p}$ das $\mathfrak{m}$ zugeordnete Primideal und $\mathfrak{g}$ ein zu $\mathfrak{m}$ elementfremdes Maximalideal, dann ist nach Satz 8 $\mathfrak{g}$ ein zu $\mathfrak{p}$ gehöriges Primärideal. Aber $\mathfrak{g}$ enthält nicht $\mathfrak{m}$ und dagegen enthalten alle verschiedenen minimalen Primär ideale das Ideal $\mathfrak{m}$. Also gibt es ein durch eins aus $q_1, \dots, q_0$ echt teilbares Primärideal. Das ist unmöglich; also wird

$$(0) = [q_1, \dots, q_0].$$

Wenn $\mathfrak{R}^2 = \mathfrak{R}$ ist, so wird $\mathfrak{R} = q_0$; also wird auch $(0) = [q_1, \dots, q_m]$ und die Darstellung ist offenbar die kürzeste.

Im anderen Falle enthält $\mathfrak{R}$ einen Totalnullteiler n ausser Null, und n soll durch alle $q_1, q_2, \dots, q_m$ teilbar sein; damit ist $(0) = [q_1, q_2, \dots, q_m, q_0]$. Da $\mathfrak{R}^n = q_0$ ist so ist klar, dass die Darstellung die kürzeste ist.

Zusatz 2. Sei $(0) = [q_1, \dots, q_m, q_0]$ eine kürzeste Darstellung mit minimalen Primär idealen und seien

$$\mathfrak{d}_i = [q_1, \dots, q_{i-1}, q_{i+1}, \dots, q_m] \quad (i=0, 1, \dots, m).$$

Dann werden

$$[\mathfrak{d}_i, q_i] = (0), \quad \mathfrak{R} = \mathfrak{d}_i + q_i \quad (i=0, 1, \dots, m)$$

Denn, wenn $i \neq 0$ ist, so sind $\mathfrak{d}_i$ nicht nilpotent, da $q_1 \dots q_{i-1} q_{i+1} \dots q_m \equiv 0 \pmod{\mathfrak{d}_i}$ sind. Damit enthalten $\mathfrak{d}_i$ idempotente Elemente e_i und $q_i = (0) : (e_i)$ sind, da für jedes n $e_i^n \equiv 0 \pmod{q_i}$ und q_i Primär ideale sind. Ferner spielen e_i damit in bezug auf $\mathfrak{d}_i$ eine Rolle von Einheitselement; also folgen daraus

$$\mathfrak{R} = \mathfrak{d}_i + q_i \quad (i=1, 2, \dots, m).$$

Wenn $i=0$ ist, enthält q_0 ein Einheitsselement e_0 in bezug auf q_0 , da $q_0^2=q_0$ ist. Weiter ist $d_0=(0):(e_0)$, sonst würde $q_0 d=(0)$ für ein Element d ausserhalb eines Primärideals etwa q_j ($j \neq 0$). Das führt uns in einen Widerspruch, weil q_0 ein Element ausserhalb des zu q_j gehörigen Primideals p_j enthält. Hiermit erhalten wir auch

$$\mathfrak{R} = d_0 + q_0 .$$

Daraus folgt ohne weiteres

Zusatz 3. *Das Nullideal lässt eine und nur eine kürzeste Darstellung als kleinstes gemeinsames Vielfaches von den zu verschiedenen Primidealen gehörigen Primärideal zu⁽¹⁾.*

Satz 9. *Sei $m_{01}, \dots, m_{0n_0}; m_{11}, \dots, m_{1n_1}; \dots; m_{i1}, \dots, m_{in_i}; \dots; m_{m1}, m_{m2}, \dots, m_{mn_m}$ ein System von unabhängigen Minimalidealen aus $\mathfrak{R}$. Seien p_i die $m_{i1}, m_{i2}, \dots, m_{in_i}$ zugeordneten Primideale und seien auch g_{ij} die zu m_{ij} elementfremden Maximalideale, welche alle anderen Minimalideale ausser m_{ij} enthalten. Dann werden*

$$q_i = [g_{i1}, g_{i2}, \dots, g_{in_i}] \quad (i=0, 1, 2, \dots, m),$$

wo q_i die zu p_i gehörigen minimalen Primärideale bedeuten.

Beweis. Nach Satz 8 sind $g_{i1}, g_{i2}, \dots, g_{in_i}$ die zu p_i gehörigen Primärideal. Damit sind die zu p_i gehörigen minimalen Primärideale q_i durch $g_{i1}, g_{i2}, \dots, g_{in_i}$ teilbar; also werden

$$q_i \equiv 0 \quad (q'_i = [g_{i1}, \dots, g_{in_i}]) \quad (i=0, 1, \dots, m).$$

Wenn $q'_i \neq 0$ (q_i) sind, so geben es in q'_i ausserhalb q_i Minimalideale m'_i derart, dass $p_i=(0):m'_i$ sind, da nach Zusatz 2 unter Satz 8 $\mathfrak{R} = d_i + q_i$ sind. Ferner sind m'_i damit durch $\mathfrak{M}_i = m_{i1} + m_{i2} + \dots + m_{in_i}$ teilbar. Andererseits ist kein Ideal aus $m_{i1}, m_{i2}, \dots, m_{in_i}$ durch q'_i teilbar und folglich werden nach den Eigenschaften von g_{ij}

$$[\mathfrak{M}_i, q'_i] = (0) .$$

Daraus folge $m'_i \neq 0$ (q'_i) mit Widerspruch. Hiermit müssen $q_i = q'_i$ sein.

Zusatz. *Wenn g_i die zu $\mathfrak{M}_i$ elementfremden Maximalideale sind, so werden auch*

$$g_i = [g_{i1}, g_{i2}, \dots, g_{in_i}] .$$

(1) Vgl. E. Noether, Abstrakter Aufbau der Idealtheorie. §7.

Denn wie beim Beweis von Satz 8 können wir beweisen, dass $\mathfrak{g}_i$ auch Primär ideale sind. Hieraus folgen, wie bei Satz 9 $\mathfrak{g}_i = \mathfrak{q}_i$; also werden $\mathfrak{g}_i = [\mathfrak{g}_{i1}, \mathfrak{g}_{i2}, \dots, \mathfrak{g}_{in_i}]$.

§ 4. Ueber eindeutige Darstellbarkeit des Nullideals als Durchschnitt der irreduziblen Ideale

Bevor wir uns zum eigentlichen Gegenstande dieses Paragraphen wenden, wollen wir folgende Hilfssätze nachweisen:

Hilfssatz 1. *Sind $m_1, m_2, \dots, m_n$ ein System der unabhängigen Minimalideale derart, dass alle Minimalideale aus $\mathfrak{R}$ durch $m_1 + m_2 + \dots + m_n$ teilbar sind, und wenn $\mathfrak{g}_i$ die zu m_i elementfremden Maximalideale, die alle anderen Minimalideale des Systems enthalten, sind, so wird*

$$(0) = [\mathfrak{g}_1, \mathfrak{g}_2, \dots, \mathfrak{g}_n]$$

eine kürzeste Darstellung des Nullideals als Durchschnitt der irreduziblen.

Denn $\mathfrak{g}_i$ sind offenbar irreduzibel. Wenn

$$\mathfrak{d} = [\mathfrak{g}_1, \mathfrak{g}_2, \dots, \mathfrak{g}_n] \neq (0)$$

wäre, so würde für ein Element m von einem durch $\mathfrak{d}$ teilbaren Minimalideal m

$$m = m_1 + m_2 + \dots + m_n,$$

wobei m_i die Elemente aus m_i sind. Damit würde

$$m_1 = m - (m_2 + \dots + m_n) \equiv 0 \pmod{\mathfrak{g}_1}$$

mit Widerspruch; also muss $\mathfrak{d} = (0)$ sein. Ferner sind m_i durch $[\mathfrak{g}_1, \dots, \mathfrak{g}_{i-1}, \mathfrak{g}_{i+1}, \dots, \mathfrak{g}_n]$ aber nicht durch $\mathfrak{g}_i$ teilbar, womit die Darstellung auch eine kürzeste ist. Natürlich ist die Darstellung auch reduziert.

Hilfssatz 2. *Ist der $\mathfrak{R}$ entsprechende gr. gem. Teiler $\mathfrak{M}_0 = m_{01} + m_{02} + \dots + m_{0n_0}$ zyklisch, so sind die zu m_{0j} elementfremden Maximalideale $\mathfrak{g}_j$ eindeutig bestimmt.*

Beweis. Nach Satz 8 sind $\mathfrak{g}_j$ die zu $\mathfrak{R}$ gehörigen Primär ideale, damit ist das zu $\mathfrak{R}$ gehörige minimale Primär ideal $\mathfrak{g}_0$ durch $\mathfrak{g}_j$ teilbar. Nach Zusatz 2 (Satz 8) ist auch

$$\mathfrak{R} = \mathfrak{d}_0 + \mathfrak{q}_0 . \quad (1)$$

Seien nun $\mathfrak{g}_j, \mathfrak{g}'_j$ zwei zu $\mathfrak{m}_{0j}$ elementefremde verschiedene Maximalideale. Dann werden

$$m_j = g_j - g'_j \neq 0, \quad g_j \notin 0 \ (\mathfrak{g}'_j), \quad g'_j \notin 0 \ (\mathfrak{g}_j), \quad (2)$$

wobei m_j, g_j, g'_j die Elemente aus $\mathfrak{m}_{0j}$, $\mathfrak{g}_j, \mathfrak{g}'_j$ sind. Da $\mathfrak{R} \cap \mathfrak{m}_{0j} = (0)$, $\mathfrak{q}_0^2 = \mathfrak{q}_0$ sind, so soll $\mathfrak{m}_{0j} \equiv 0 \ (\mathfrak{d}_0)$ sein. Damit folgen wegen (1), (2)

$$m_j = d_j - d'_j, \quad g_j = d_j + q_0, \quad g'_j = d'_j + q_0, \quad d_j \neq 0, \quad d'_j \neq 0 \quad (3)$$

wobei d_j, d'_j die Elemente aus $\mathfrak{d}_0$ sind und q_0 ein Element aus $\mathfrak{q}_0$ ist, da $[\mathfrak{g}_j, \mathfrak{g}'_j] \supseteq \mathfrak{q}_0$ ist.

Da $\mathfrak{R}^p \equiv 0 \ (\mathfrak{q}_0)$ ist, so soll $\mathfrak{d}_0^p = (0)$ sein, damit enthält $\mathfrak{d}_0$ nur endlich viele verschiedene Elemente. Daraus folgen

$$s d_j = 0, \quad s' d'_j = 0$$

für endliche ganze Zahlen s, s' , und es sein auch die Zahlen die Grade von d_j, d'_j . Ferner folgen aus (3)

$$s m_j = -s d'_j, \quad s' m_j = s' d_j .$$

Da $[\mathfrak{m}_{0j}, \mathfrak{g}'_j] = (0)$, $[\mathfrak{m}_{0j}, \mathfrak{g}_j] = (0)$ sind, so müssen $s m_j = s' m_j = 0$ sein. Andererseits ist für eine Primzahl p $p m_j = 0$, weil $\mathfrak{m}_{0j}$ ein Minimalideal ist. Daraus folgen

$$s = s_1 p, \quad s' = s'_1 p, \quad p m_j = 0 \quad (4)$$

Ferner gibt es ein $\mathfrak{R}$ zugeordnetes Minimalideal von der Form

$$(s_1 d_j), \quad \text{oder} \quad (s_1 d_j d''_j),$$

wo d''_j ein Element aus $\mathfrak{d}_0$ ist. Die Grade der Elemente aus $\mathfrak{m}_{0j}$, $(s_1 d_j)$ und $(s_1 d_j d''_j)$ sind p . Nach der Voraussetzung ist $\mathfrak{M}_0$ aber zyklisch, daraus folgt wegen Satzes 3

$$\mathfrak{m}_{0j} = (s_1 d_j), \quad \text{oder} \quad \mathfrak{m}_{0j} = (s_1 d_j d''_j) .$$

Also wird $\mathfrak{m}_{0j} \equiv 0 \ (\mathfrak{g})$ mit Widerspruch. Hiermit muss $\mathfrak{g}_j = \mathfrak{g}'_j$ sein.

Satz 10. *Damit die kürzeste Darstellung des Nullideals als kleinstes gemeinsames Vielfaches von irreduziblen Idealien eindeutig bestimmt ist, ist notwendig und hinreichend, dass alle $\mathfrak{M}_i$ ($i \neq 0$) Minimalideale sind und $\mathfrak{M}_0$ zyklisch oder Nullideal ist.*

Beweis. Die Bedingung ist hinreichend. Denn, wenn

$$(0)=[r_1, r_2, \dots, r_n]=[r'_1, r'_2, \dots, r'_n]$$

zwei kürzeste Darstellungen als kleinstes gemeinsames Vielfaches von irreduziblen sind, so sind die Anzahl der Komponenten gleich der Anzahl n der unabhängigen Minimalideale.

Wir setzen nun :

$$d_i=[r_1, r_2, \dots, r_{i-1}, r_{i+1}, \dots, r_n], \quad d'_i=[r'_1, \dots, r'_{i-1}, r'_{i+1}, \dots, r'_n].$$

Ferner seien m_i, m'_i die durch d_i, d'_i teilbaren Minimalideale, so werden nach Satz 7 m_i unabhängig voneinander und ebenso sind m'_i auch unabhängig voneinander, und alle Minimalideale aus $\mathfrak{R}$ sind durch $m_1 + \dots + m_n, m'_1 + \dots + m'_n$ teilbar. Nach der Voraussetzung und Satz 3 folgt, dass das System m'_i identisch mit dem System m_i ist. Also können wir

$$m_i=m'_i \quad (i=1, 2, \dots, n)$$

setzen. Andererseits sind r_i die zu m_i elementfremden Maximalideale, die alle anderen unabhängigen Minimalideale ausser m_i enthalten, sonst würden r_i reduzibel.

Damit folgen wegen Satzes 9 und Hilfssatzes 2

$$r_1=r'_1, r_2=r'_2, \dots, r_n=r'_n.$$

Die Bedingung ist aber auch notwendig. Denn, wenn etwa $\mathfrak{M}_1$ nicht Minimalideal oder nicht zyklisch ist, so ist nach Satz 3 und Zusatz (Satz 4) die Darstellung von $\mathfrak{M}_1$ als direkte Summe der Minimalideale nicht eindeutig bestimmt. Also können wir zwei verschiedene System von unabhängigen Minimalidealen

$$m_1, m_2, \dots, m_n; \quad m'_1, m'_2, \dots, m'_n$$

finden, sodass

$$m'_1=(m_1-m_2), \quad m'_i=m_i \quad (i=2, 3, \dots, n),^{(1)}$$

wobei m_1, m_2 die Elemente von m_1, m_2 sind, die zu $\mathfrak{M}_1$ gehören. Daraus erhalten wir wegen Hilfssatzes 1 eine kürzeste Darstellung des Nullideals

$$(0)=[g_1, g_2, \dots, g_n],$$

(1) Wenn $\mathfrak{M}_1$ einen von $\mathfrak{R}$ verschiedenen Primideal entspricht, so folgt nach Zusatz 2 (Satz 8), Satz 9 $\mathfrak{R}(m_1-m_2)=(m_1-m_2)$.

wobei $\mathfrak{g}_i$ die zu $\mathfrak{m}_i$ elementfremden Maximalideale sind, die alle anderen Minimalideale ausser $\mathfrak{m}_i$ enthalten.

Andererseits können wir $\mathfrak{g}_i$ ($i=3, 4, \dots, n$) als die zu $\mathfrak{m}$ elementfremden Maximalideale betrachten, damit erhalten wir auch eine andere kürzeste Darstellung

$$(0) = [\mathfrak{g}'_1, \mathfrak{g}'_2, \mathfrak{g}_3, \dots, \mathfrak{g}_n].$$

In den beiden kürzesten Darstellungen sind offenbar $\mathfrak{g}'_2 \neq \mathfrak{g}_i$ ($i \neq 2$). Dazu wird auch $\mathfrak{g}'_2 \neq \mathfrak{g}_2$; sonst würde wegen $\mathfrak{m}'_1 = (\mathfrak{m}_1 - \mathfrak{m}_2)$

$$\mathfrak{m}_2 \equiv 0 \ (\mathfrak{g}_2)$$

mit Widerspruch. Also erhalten wir zwei verschiedene kürzeste Darstellungen.

Satz 11. *Damit alle minimalen Primärideale irreduzibel sind, ist notwendig und hinreichend, dass die Anzahl der unabhängigen Minimalideale aus $\mathfrak{R}$ gleich der Anzahl der Minimalidealklassen ist.*

Beweis. Nach Satz 4 ist die Anzahl der unabhängigen Minimalideale nicht kleiner als die Anzahl der Minimalidealklassen. Wenn die Anzahl der unabhängigen Minimalideale grösser als die Anzahl der Klassen ist, so geben es wenigstens zwei verschiedene unabhängige Minimalideale, die demselben Primideal $\mathfrak{p}_i$ zugeordnet sind. Nach Satz 9 ist damit das zu $\mathfrak{p}_i$ gehörige minimale Primärideal $\mathfrak{q}_i$ reduzibel.

Wenn ein minimales Primärideal reduzibel ist, so wird in einer kürzesten Darstellung

$$(0) = [\mathfrak{r}_1, \mathfrak{r}_2, \dots, \mathfrak{r}_n]$$

die Anzahl der irreduziblen Ideale grösser als die Anzahl der Klassen, da nach Zusatz 2 unter Satz 8 $(0) \neq [\mathfrak{q}_1, \dots, \mathfrak{q}'_i, \dots, \mathfrak{q}_m, \mathfrak{q}_0]$ ist, wenn $\mathfrak{q}'_i$ ein echter Teiler von $\mathfrak{q}_i$ ist, und da alle irreduziblen Ideale $\mathfrak{r}_i$ ein minimales Primärideal enthalten. Damit ist nach Satz 7 die Anzahl der unabhängigen Minimalideale grösser als die Anzahl der Minimalidealklassen. Hiermit ist der Satz bewiesen.

§ 5. Einige Eigenschaften der direkten Summen

Der Ring $\mathfrak{R}$ ist als direkte Summe von der Form

$$\mathfrak{R} = \mathfrak{R}_1 + \mathfrak{R}_2 + \dots + \mathfrak{R}_m + \mathfrak{R}'$$

darstellbar, wobei $\mathfrak{R}_i$ die speziellen primären Ringe oder Körper sind und $\mathfrak{R}'$ ein endlicher nilpotenter Ring ist. $\mathfrak{R}'$ ist auch gleich dem

Idealquotient (0): $\mathfrak{q}_0$; wo $\mathfrak{q}_0$ das zu $\mathfrak{R}$ gehörige minimale Primärideal ist. Und dabei sind die Ringe $\mathfrak{R}_i, \mathfrak{R}'$ eindeutig bestimmt,⁽¹⁾ damit hängt die eindeutige Darstellbarkeit von $\mathfrak{R}$ als direkte Summe der direkt-unzerlegbaren Ringe von der Eigenschaft des endlichen nilpotenten Ringes $\mathfrak{R}'$ ab. Deshalb werden wir im folgenden einen vollständigen Ueberblick über die Darstellbarkeit von $\mathfrak{R}'$ als direkte Summe von direkt-unzerlegbaren Ringen gewinnen.

Die Gesamtheit $\mathfrak{R}'_1$ aller Elemente aus $\mathfrak{R}'$, deren Grade Potenzen einer Primzahl p_1 sind, bildet ein Ideal. Existieren in $\mathfrak{R}'$ noch die Elemente, deren Grade Potenzen von p_2 ($\neq p_1$) sind, so erhalten wir auch ein Ideal $\mathfrak{R}'_2$ und

$$[\mathfrak{R}'_1, \mathfrak{R}'_2] = (0).$$

So fortfahrend erhalten wir die endlich vielen Ideale

$$\mathfrak{R}'_1, \mathfrak{R}'_2, \dots, \mathfrak{R}'_r,$$

die die Beziehungen $[\mathfrak{R}'_i, (\mathfrak{R}'_1, \dots, \mathfrak{R}'_{i-1}, \mathfrak{R}'_{i+1}, \dots, \mathfrak{R}'_r)] = (0)$ erfüllen. Sei nun r' ein beliebiges Element aus $\mathfrak{R}'$ und sei $p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$ der Grad von r' . Da wir die ganzen Zahlen $s_1, s_2, \dots, s_r$ bestimmen können, sodass

$$\begin{aligned} 1 &= s_1 p_2^{a_2} \dots p_r^{a_r} + s_2 p_1^{a_1} p_3^{a_3} \dots p_r^{a_r} + \dots + s_r p_1^{a_1} \dots p_{r-1}^{a_{r-1}}, \\ (s_i, p_i^{a_i}) &= 1 (i=1, \dots, r), \end{aligned}$$

so wird

$$r' = s_1 p_2^{a_2} \dots p_r^{a_r} r' + s_2 p_1^{a_1} p_3^{a_3} \dots p_r^{a_r} r' + \dots + s_r p_1^{a_1} \dots p_{r-1}^{a_{r-1}} r'$$

und die Grade der Elemente $s_i p_1^{a_1} \dots p_{i-1}^{a_{i-1}} p_{i+1}^{a_{i+1}} \dots p_r^{a_r} r'$ sind die Primzahlpotenzen $p_i^{a_i}$. Daraus folgt also

$$\mathfrak{R}' = \mathfrak{R}'_1 + \mathfrak{R}'_2 + \dots + \mathfrak{R}'_r$$

Ferner ist die Darstellung offenbar eindeutig bestimmt.⁽²⁾

Es liegt die Frage nahe, ob es möglich ist, die Ringe $\mathfrak{R}'_i$ eindeutig noch zu zerlegen. Dazu brauchen wir zunächst den folgenden Hilfssatz nachzuweisen

Hilfssatz. Ist $\mathfrak{R}''$ ein endlicher nilpotenter Ring, in dem der Grad jedes Elements eine Potenz einer Primzahl p ist, und ist $\mathfrak{R}''$ direkt

(1) S. Mori, Ueber Primär ideale in kommutativen Ringbereichen.

(2) Vgl. K. Shoda, Ueber die Einheitsgruppe eines endlichen Ringes, Math. Ann. 102, S. 279.

zerlegbar, so stattfindet nicht die Eindeutigkeit der Darstellung von $\mathfrak{R}''$ als direkte Summe der direkt-unzerlegbaren Ringe.

Beweis. Sei nun $\mathfrak{R}'' = \mathfrak{R}'_1 + \mathfrak{R}'_2 + \dots + \mathfrak{R}'_l$, wo $\mathfrak{R}'_i$ direkt-unzerlegbar sind.

$\mathfrak{R}'_1$ ist als grösster gemeinsamer Teiler $((r_1), (r_2), \dots, (r_l))$ von Hauptidealien (r_i) aus $\mathfrak{R}''$ darstellbar, und solche verschiedene Darstellungen sind auch endlich. Wenn die Anzahl der Hauptideale in der Darstellung am kleinsten ist, dann heissen die Elemente $r_1, r_2, \dots, r_l$ eine Basis von $\mathfrak{R}'_1$.

Wenn $r_1, r_2, \dots, r_l$ eine Basis von $\mathfrak{R}'_1$ ist, so ist es nicht möglich, r_i in der Form darzustellen

$$r_i = \varphi_i(r_1, r_2, \dots, r_l) \quad (i=1, 2, \dots, l),$$

wobei φ_i die Polynome mit ganzen rationalen Koeffizienten bedeuten, die kein von $r_1, \dots, r_l$ freies Glied und kein lineares Glied von r_i enthalten.

Wenn die Beziehung möglich wäre, so würde

$$r_i = r_i \varphi'_i(r_1, \dots, r_l) + \varphi''_i(r_1, \dots, r_{i-1}, r_{i+1}, \dots, r_l),$$

wobei φ'_i, φ''_i kein von $r_1, \dots, r_l$ freies Glied enthalten. Also würden daraus

$$\begin{aligned} r_i &= (r_i \varphi'_i + \varphi''_i) \varphi'_i + \varphi''_i \\ r_i &= (r_i \varphi'_i + \varphi''_i) \varphi_i'^2 + \varphi'_i \varphi_i'' + \varphi_i'' \\ &\dots\dots\dots \\ &\dots\dots\dots \\ r_i &= r_i \varphi_i'^n + \varphi_i'^{n-1} \varphi_i'' + \dots + \varphi_i' \varphi_i'' + \varphi_i'' . \end{aligned}$$

Da $\mathfrak{R}'_1$ ein nilpotenter Ring ist, so würde für hinreichend grosse Zahl n

$$\varphi_i'^n = 0 .$$

Damit würde

$$r_i \equiv 0 ((r_1), \dots, (r_{i-1}), (r_{i+1}), \dots, (r_l))$$

im Widerspruch mit der Eigenschaft der Basis.

Es sei

$$\mathfrak{R}'_1 = ((r_1), (r_2), \dots, (r_l)),$$

wo r_i eine Basis von $\mathfrak{R}'_1$ sind, und sei m auch ein Element eines Minimalideals $\mathfrak{m}$ aus $\mathfrak{R}''_2$. Dann ist m ein Totalnullteiler von $\mathfrak{R}''$. Es sei ein folgendes Ideal gebildet:

$$\mathfrak{R}'''_1 = ((r_1 + m), (r_2), \dots, (r_l)).$$

Dann hat das Ideal die folgenden Eigenschaften:

$$\text{I.} \quad \mathfrak{R}'''_1 \neq \mathfrak{R}''_1, [\mathfrak{R}'''_1, \mathfrak{R}''_i] = (0) \quad (i=2, 3, \dots, k).$$

Wenn $r_1 \equiv 0 \pmod{\mathfrak{R}'''_1}$ ist, so soll

$$\begin{aligned} r_1 = & (r_1 + m)^n f_0(r_1, \dots, r_l) + (r_1 + m)^{n-1} f_1(r_1, \dots, r_l) + \dots \\ & + (r_1 + m) f_{n-1}(r_1, \dots, r_l) + f_n(r_1, \dots, r_l) \end{aligned}$$

sein. Dabei enthält $f_n(r_1, \dots, r_l)$ kein lineares Glied von r_1 und kein von r_i freies Glied, und ferner sind $f_0 \dots f_n$ Polynome mit ganzen rationalen Koeffizienten, da $\mathfrak{R}''$ nilpotent ist. Also wird

$$\begin{aligned} r_1 = & r_1^n f_0(r_1, \dots, r_l) + r_1^{n-1} f_1(r_1, \dots, r_l) + \dots \\ & + (r_1 + m) f_{n-1}(r_1, \dots, r_l) + f_n(r_1, \dots, r_l) \end{aligned}$$

Sei nun s ein ganzzahliges Glied von $f_{n-1}(r_1, \dots, r_l)$, dann wird

$$r_1 - sr_1 = sm + \varphi(r_1, \dots, r_l)$$

wo φ ein Polynom mit ganzen rationalen Koeffizienten bedeutet, das kein von r_i freies Glied und kein lineares Glied von r_1 enthält.

Da $[\mathfrak{R}'_1, \mathfrak{R}''_2] = (0)$ ist, so soll $sm = 0$ sein, also ist s durch p teilbar und $(s-1, p) = 1$. Andererseits ist der Grad von r_1 eine Potenz von p . Damit ist für eine ganze Zahl t

$$r_1 = t\varphi(r_1, \dots, r_l),$$

wo φ kein lineares Glied von r_1 und kein von r_i freies Glied enthält. Das ist aber unmöglich.

Hiermit soll $r_1 \not\equiv 0 \pmod{\mathfrak{R}'''_1}$ sein. Daraus folgt sofort die Behauptung.

$$\text{II.} \quad \mathfrak{R}'''_1 + \mathfrak{R}''_2 = \mathfrak{R}'_1 + \mathfrak{R}''_2.$$

III. $\mathfrak{R}'''_1$ ist direkt-unzerlegbar. Denn $\mathfrak{R}'_1$ ist ringisomorph mit $\mathfrak{R}''_1$.

Damit ist dann der Hilfssatz bewiesen.

Zusammenfassend kommt

Satz 12. *Der Ring $\mathfrak{R}$ ist dann und nur dann als direkte Summe von direkt-unzerlegbaren Ringen eindeutig darstellbar, wenn jede Gesamtheit aller Elemente von (0) : q_0 , deren Grade Potenzen einer Primzahl sind, stets direkt-unzerlegbar ist. Dabei ist q_0 das zu $\mathfrak{R}$ gehörige minimale Primärideal.*

Satz 13. *Für ein Primideal $\mathfrak{p}$ aus $\mathfrak{R}$ gebe es kein Ideal zwischen $\mathfrak{p}$ und $\mathfrak{p}^2$, dann gibt es auch kein Ideal zwischen $\mathfrak{p}^n$ und $\mathfrak{p}^{n+1}$ für jedes n .⁽¹⁾*

Beweis. Es sei etwa α ein erstes Ideal, das zwischen zwei Potenzen des Primideals $\mathfrak{p}$ liegt und sei auch $\mathfrak{p}^m > \alpha > \mathfrak{p}^{m+1}$. Dann erhalten wir eine Hauptkompositionsreihe

$$\mathfrak{p}, \mathfrak{p}^2, \dots, \mathfrak{p}^m, \dots, \alpha, \dots, \mathfrak{p}^{m+1}.$$

Der Restklassenring $\mathfrak{R}' = \mathfrak{R}/\mathfrak{p}^2$ enthält nur ein einziges Primideal $\mathfrak{p}'$, das $\mathfrak{p}$ entspricht und von $\mathfrak{R}'$ verschieden ist, und wenn $\mathfrak{R} = \mathfrak{p}$ ist, so ist $\mathfrak{R}'$ ein einziges Primideal. Damit ist $\mathfrak{R}'$ in der Form zerlegbar

$$\mathfrak{R}' = \mathfrak{m}_1 + \mathfrak{m}, \quad \mathfrak{R}' = \mathfrak{m}_1 \quad \text{oder} \quad \mathfrak{R}' = \mathfrak{m},$$

wo $\mathfrak{m}_1$ ein Körper oder ein spezieller primärer Ring und $\mathfrak{m}$ ein nilpotenter Ring ist.

Wenn $\mathfrak{m}_1$ ein primärer Ring ist und wenn $\mathfrak{R}' = \mathfrak{m}_1 + \mathfrak{m}$ ist, so existiert ein Ideal zwischen $\mathfrak{p}'$ und (0) . Das ist aber unmöglich. Damit erhalten wir zwei Fälle

- I. $\mathfrak{R}' = \mathfrak{m}_1$ ($\mathfrak{m}_1$ primärer Ring)
- II. $\mathfrak{R}' = \mathfrak{m}$ oder $\mathfrak{R}' = \mathfrak{m}_1 + \mathfrak{m}$ ($\mathfrak{m}_1$ Körper).

Im ersten Falle ist $\mathfrak{R}/\mathfrak{p}$ wegen des Isomorphiesatzes ein Körper und $\mathfrak{R}\mathfrak{p} \cong 0$ ($\mathfrak{p}^2$).

Also wird nach Sonoscher Methode

$$\mathfrak{p} = (\mathfrak{R}\mathfrak{p}, \mathfrak{p}^2), \quad \mathfrak{p}\mathfrak{p} \cong 0 \quad (\mathfrak{p}^2),$$

wo $\mathfrak{p}$ ein Element aus $\mathfrak{p}$ ausserhalb $\mathfrak{p}^2$ ist. Daraus folgt nach dem distributiven Gesetz:

$$\mathfrak{p}^m = (\mathfrak{R}\mathfrak{p}^m, \mathfrak{p}^{m+1}), \quad \mathfrak{p}^m\mathfrak{p} \cong 0 \quad (\mathfrak{p}^{m+1}).$$

(1) Der Satz unter Voraussetzung der Existenz des Einheitselements findet sich bei M. Sono. On Congruences II. Memoirs of the College of Science Kyoto Imperial University (1918). Vgl. E. Noether, Abstrakter Aufbau der Idealtheorie, § 8.

Für jedes Element a aus $\mathfrak{A}$ ausserhalb $\mathfrak{p}^{m+1}$ wird auch

$$a \equiv rp^m \pmod{\mathfrak{p}^{m+1}},$$

wo r ein Element aus $\mathfrak{A}$ ausserhalb $\mathfrak{p}$ bedeutet. Da $\mathfrak{A}/\mathfrak{p}$ ein Körper ist, so gibt es stets ein Element r' derart, dass für jedes Element r' aus $\mathfrak{A}$

$$r r' \equiv r' \pmod{\mathfrak{p}}.$$

Also wird

$$\mathfrak{A}p^m \equiv 0 \pmod{\mathfrak{a}}, \quad \mathfrak{p}^m \equiv 0 \pmod{\mathfrak{a}}.$$

Im anderen Fälle ist $\mathfrak{A}\mathfrak{p} \equiv 0 \pmod{\mathfrak{p}^2}$ und werden

$$\mathfrak{p} = (\mathfrak{p}, \mathfrak{p}^2), \quad \mathfrak{A}\mathfrak{p} \equiv 0 \pmod{\mathfrak{p}^2}, \quad s\mathfrak{p} \equiv 0 \pmod{\mathfrak{p}^2},$$

wo s eine Primzahl ist, da es kein Ideal zwischen $\mathfrak{p}$ und $\mathfrak{p}^2$ gibt. Daraus folgen also auch

$$\mathfrak{p}^m = (\mathfrak{p}^m, \mathfrak{p}^{m+1}), \quad \mathfrak{A}\mathfrak{p}^m \equiv 0 \pmod{\mathfrak{p}^{m+1}}, \quad s\mathfrak{p}^m \equiv 0 \pmod{\mathfrak{p}^{m+1}}.$$

Für jedes Element a aus $\mathfrak{A}$ ausserhalb $\mathfrak{p}^{m+1}$ wird

$$a \equiv s' p^m \pmod{\mathfrak{p}^{m+1}},$$

wobei die ganze Zahl s' relativ prim zu s ist. Daraus folgt auch

$$(\mathfrak{p}^m) \equiv 0 \pmod{\mathfrak{a}}, \quad \mathfrak{p}^m \equiv 0 \pmod{\mathfrak{a}}.$$

Also ist die Annahme falsch und der Satz bewiesen.

Der Satz 13 ist auch in der folgenden Form ausgesprochen.

Satz 14. *Es sei $\mathfrak{a}$ ein Teiler einer Potenz eines Primideals $\mathfrak{p}$ und sei $\mathfrak{a}$ durch $\mathfrak{p}$ teilbar. Dann ist $\mathfrak{a}$ eine Potenz von $\mathfrak{p}$, wenn es kein Ideal zwischen $\mathfrak{p}$ und $\mathfrak{p}^2$ gibt.*

Sei nun $\mathfrak{p} \nmid \mathfrak{a}$, dann folgt aus der Voraussetzung

$$\mathfrak{p}^{n+1} \equiv 0 \pmod{\mathfrak{a}}, \quad \mathfrak{p}^n \not\equiv 0 \pmod{\mathfrak{a}}, \quad \text{für eine Zahl } n (> 0).$$

Da $\mathfrak{a} \equiv 0 \pmod{\mathfrak{p}}$ ist, so können wir entweder eine Zahl m finden, sodass

$$\mathfrak{a} \equiv 0 \pmod{\mathfrak{p}^m}, \quad \mathfrak{a} \not\equiv 0 \pmod{\mathfrak{p}^{m+1}} \quad (1 \leq m < n+1),$$

oder wir erhalten $\alpha = \mathfrak{p}^{m+1}$. Wenn der erste Fall möglich wäre, so hätten wir wegen Satzes 13

$$\mathfrak{p}^m = (\alpha, \mathfrak{p}^{m+1}),$$

also würde

$$\mathfrak{p}^n = (\alpha \mathfrak{p}^{n-m}, \mathfrak{p}^{n+1}) \equiv 0 \pmod{\alpha}$$

mit Widerspruch. Damit soll $\alpha = \mathfrak{p}^{n+1}$ ($n \geq 0$) sein.

Satz 15. *Jedes Primärideal aus $\mathfrak{R}$ ist dann und nur dann irreduzibel, wenn durch jedes minimale Primärideal eine und nur eine Hauptkompositionsreihe läuft.*

Denn wenn $\mathfrak{q}$ ein zu $\mathfrak{p}_i$ gehöriges Primärideal ist, so ist $\mathfrak{q}$ auch ein Teiler des zu $\mathfrak{p}_i$ gehörigen minimalen Primärideals $\mathfrak{q}_i$. Wir erhalten daher wenigstens zwei verschiedene durch $\mathfrak{q}_i$ laufende Hauptkompositionsreihen, wenn $\mathfrak{q}$ reduzibel ist.

Existieren zwei verschiedene Hauptkompositionsreihen

$$\mathfrak{R}, \alpha_1, \alpha_2, \dots, \alpha_n, \mathfrak{q}_i \quad \text{und} \quad \mathfrak{R}, \alpha'_1, \alpha'_2, \dots, \alpha'_n, \mathfrak{q}_i,$$

so können wir zwei Ideale α_k, α'_k derart, dass

$$\alpha_k \neq \alpha'_k \quad \alpha_j = \alpha'_j \quad (j = k+1, k+2, \dots, n, n+1, \text{ wo } \alpha_{n+1} = \alpha'_{n+1} = \mathfrak{q}_i)$$

finden, sonst würden die beiden Kompositionsreihen identisch. Da $\alpha_{k+1} = [\alpha_k, \alpha'_k]$ ist, so wird α_{k+1} reduzibel. Ist das zugehörige Primärideal $\mathfrak{p}_i$ von $\mathfrak{R}$ verschieden, so soll $\mathfrak{p}_i = \alpha_1 = \alpha'_1$ sein. Ferner ist jeder Teiler eines minimalen Primärideals auch ein Primärideal. Damit ist α_{k+1} ein zu $\mathfrak{p}_i$ gehöriges Primärideal und reduzibel. Hiermit ist der Satz bewiesen.

§ 6. Ringisomorphismus der verschiedenen Zerlegungen von $\mathfrak{R}$.

Es seien $\mathfrak{R} = \alpha_1 + \alpha_2 = \mathfrak{b} + \mathfrak{c}$ zwei verschiedene Darstellungen des Ringes $\mathfrak{R}$ als direkte Summe. Sind

$$\mathfrak{b}_k^{(1)}, \mathfrak{b}_k^{(2)}, \mathfrak{b}_k^{(3)}, \dots \quad (k=1, 2)$$

die Zurückleitungen eines Elementes b aus $\mathfrak{b}$ hinsichtlich α_k ($k=1, 2$)⁽¹⁾, so ist es möglich, dass in der Reihe identische Elemente vorkommen und dabei heisst das Element b *periodisch in bezug auf α_k* .

(1) W. Krull, Ueber verallgemeinerte endliche Abelsche Gruppen, Math. Zeitschr. 23 (1925), S. 175.

Bedeutet P_k ($k=1, 2$) die Gesamtheit aller Elemente b aus $\mathfrak{b}$, die mit einer ihrer Zurückleitungen hinsichtlich α_k identisch sind, m.a.W.: b ist reinperiodisch, so stellt P_k ein Ideal von $\mathfrak{R}$ dar. Die Ideale E_k werden auch definiert als die Gesamtheit aller Elemente aus $\mathfrak{b}$, die die Eigenschaft besitzen, dass eine ihrer Zurückleitungen hinsichtlich α_k verschwindet. Aus diesen Definitionen folgt leicht

Hilfssatz. *Ist jedes Element aus $\mathfrak{b}$ periodisch inbezug auf α_k ($k=1, 2$), so werden $[P_k, E_k]=(0)$, $\mathfrak{b}=P_k+E_k$ ($k=1, 2$).*

Da jedes Element aus P_k mit einer seiner Zurückleitungen hinsichtlich α_k übereinstimmt, so ist offenbar

$$[P_k, E_k]=(0) \quad (k=1, 2).$$

Es sei nun b ein beliebiges Element aus $\mathfrak{b}$ und seien $b^{(1)}, b^{(2)}, \dots$ die Zurückleitungen von b hinsichtlich α_k . Wenn ein Glied der Reihe Null ist, so findet sich die Beziehung $b \equiv 0 (E_k)$. Im anderen Falle kommen wegen der Voraussetzung auch identische Elemente in der Reihe $b=b^{(0)}, b^{(1)}, b^{(2)}, \dots, b^{(m)}, \dots, b^{(m+n)}, \dots$ vor. Sei $b^{(m+n)}$ das erste wiederholte Element in der Reihe und sei auch $b^{(m)}=b^{(m+n)}$. Dann werden

$$b^{(m+i)}=b^{(m+n+i)}, \quad b^{(m)}=b^{(m+in)} \quad \text{für jedes } i.$$

Wir können zwei positive ganze Zahlen s, t bestimmen, sodass

$$sn=t+m, \quad 1 \leq t \leq n.$$

Betrachten wir das Element $b^{(m+t)}$, so sind seine Zurückleitungen hinsichtlich α_k

$$b^{(m+t)}, b^{(m+t+1)}, \dots, b^{(m+n+t)}=b^{(m+t)}, \dots$$

Damit ist also $b^{(m+t)}$ ein Element aus P_k . Nun wird $b^{(0)}-b^{(m+t)}$ auch ein Element aus $\mathfrak{b}$, dessen Zurückleitungen hinsichtlich α_k

$$b^{(0)}-b^{(m+t)}, b^{(1)}-b^{(m+t+1)}, \dots, b^{(m)}-b^{(m+t+m)},$$

sind. Da $b^{(m+t+m)}=b^{(m+sn)}=b^{(m)}$ aber ist, so ist das Element $b^{(0)}-b^{(m+t)}$ in E_k enthalten. Hieraus folgt $\mathfrak{b} \equiv 0 (P_k+E_k)$ und der Hilfssatz ist bewiesen.

Satz 16. *Ist $\mathfrak{R}=\alpha_1+\alpha_2=\mathfrak{b}+\mathfrak{c}$, so wird*

$$\mathfrak{b}=P_1+E_1=P_2+E_2.$$

Beweis: Wegen des Zusatzes 2 unter Satz 8 haben wir

$$\mathfrak{R} = \mathfrak{q}_0 + \mathfrak{d}_0,$$

wo $\mathfrak{d}_0$ ein endliches nilpotentes Ideal ist, $\mathfrak{q}_0$ das zu $\mathfrak{R}$ gehörige minimale Primärideal und $\mathfrak{q}_0$ auch ein Einheitsselement e_0 in bezug auf selbst enthält. Somit ist jedes Element b aus $\mathfrak{b}$ in der Form $b = q_0 + d_0$ darstellbar, und ferner $e_0 = a_1 + a_2$, wo a_1 bzw. a_2 Element aus $\mathfrak{a}_1$ bzw. $\mathfrak{a}_2$ ist. Daraus folgt $(a_1 + a_2)b = e_0 q_0 = q_0$; also sind q_0 und d_0 gleichzeitig in $\mathfrak{b}$ enthalten.

Wird unter b_1 bzw. b_2 ein Element aus $\mathfrak{d}_1 = [\mathfrak{a}_1, \mathfrak{b}]$ bzw. $\mathfrak{d}_2 = [\mathfrak{a}_2, \mathfrak{b}]$ verstanden, so wird $q_0 = b_1 + b_2$. Die Zurückleitung von b_1 bzw. b_2 hinsichtlich $\mathfrak{a}_1$ ist b_1 bzw. 0 und seine Zurückleitung hinsichtlich $\mathfrak{a}_2$ auch 0 bzw. b_2 . Nämlich sind b_1 und b_2 periodisch.

Es bezeichne nun $\bar{\mathfrak{d}}_0 = [\bar{\mathfrak{d}}_0, \mathfrak{b}]$, dann ist die Zurückleitung $\bar{d}_{0k}^{(1)}$ jedes Elementes $\bar{d}_0$ aus $\bar{\mathfrak{d}}_0$ hinsichtlich $\mathfrak{a}_k$ auch in $\bar{\mathfrak{d}}_0$ enthalten, denn aus der Beziehung $\bar{d}_0 = a_1 + a_2$, $a_1 = \bar{d}_{01}^{(1)} + c$, $a_2 = \bar{d}_{02}^{(1)} - c$ folgen $e_0 a_1 = e_0 a_2 = 0$, $e_0 \bar{d}_{01}^{(1)} = e_0 \bar{d}_{02}^{(1)} = e_0 c = 0$, da $[\mathfrak{a}_1, \mathfrak{a}_2] = (0)$, $[\mathfrak{b}, \mathfrak{c}] = (0)$ sind. Wegen der Endlichkeit von $\mathfrak{d}_0$ ist $\bar{\mathfrak{d}}_0$ auch endlich und jedes Element aus $\bar{\mathfrak{d}}_0$ muss daher periodisch sein. Hiermit ist jedes Element b aus $\mathfrak{b}$ auch periodisch, und aus dem Hilfssatz folgt der Satz.⁽¹⁾

Wenn $\mathfrak{d}_k = [\mathfrak{a}_k, \mathfrak{b}]$ ($k=1, 2$) vom Nullideal verschieden ist, so werden P_1, E_1 auch vom Nullideal verschieden. Denn die Zurückleitung jedes Elementes von $\mathfrak{d}_1$ hinsichtlich $\mathfrak{a}_1$ ist mit selbst identisch, und die Zurückleitung jedes Elementes von $\mathfrak{d}_2$ hinsichtlich $\mathfrak{a}_1$ ist Null, daraus folgen $\mathfrak{d}_1 \equiv 0 (P_1)$, $\mathfrak{d}_2 \equiv 0 (E_1)$. Wegen des Satzes kommt somit

Zusatz. Wenn $\mathfrak{R} = \mathfrak{a}_1 + \mathfrak{a}_2 = \mathfrak{b} + \mathfrak{c}$, $[\mathfrak{a}_k, \mathfrak{b}] \neq (0)$ ($k=1, 2$) sind, so ist $\mathfrak{b}$ direkt zerlegbar.

Hilfssatz 1. Ist $\mathfrak{R} = \mathfrak{a}_1 + \mathfrak{a}_2 = \mathfrak{a}_1 + \mathfrak{c}$, so ist $\mathfrak{a}_2$ zu $\mathfrak{c}$ ringisomorph.

Es sei $a (\neq 0)$ ein beliebiges Element aus $\mathfrak{a}_2$, dann wird

$$a_2 = a_1 + c, \quad c \neq 0 \tag{1}$$

Damit werden wir dem Element a_2 das Element c aus $\mathfrak{c}$ zuordnen. Umgekehrt wird auch $c = a'_1 + a'_2$, $a'_2 \neq 0$; daraus folgt aber

$$a_2 - a'_2 = a_1 + a'_1, \quad a_2 = a'_2.$$

(1) Zufolge des Beweises können wir leicht bemerken, dass E_k ein Ideal, das nur endlich viele Elemente besitzt, ist, wenn $[\mathfrak{a}_k, \mathfrak{b}] = (0)$ ($k=1, 2$ ist; da $\mathfrak{b}$ durch $\mathfrak{d}_0$ teilbar wird. Wenn $\mathfrak{R}$ Einheitsselement enthält, so werden $\mathfrak{b} = \mathfrak{d}_1 + \mathfrak{d}_2$, $\mathfrak{d}_1 = P_1 = E_2$, $\mathfrak{d}_2 = P_2 = E_1$.

Also ist die Zuordnung der Elemente a_2 und c umkehrbar eindeutig; nämlich wird $a_2 \simeq c$.

Für ein anderes Element $\bar{a}_2$ aus α_2 wird auch

$$\bar{a}_2 = \bar{a}_1 + \bar{c}, \quad \bar{a}_2 \simeq \bar{c} \quad (2)$$

Wegen (1), (2) folgt $a_2 \bar{a}_2 = a_1 \bar{a}_1 + c \bar{c}$.

Hiermit ist bei unserer Zuordnung auch

$$a_2 \bar{a}_2 \simeq c \bar{c}.$$

Ferner ist klar $a_2 + \bar{a}_2 \simeq c + \bar{c}$. Damit sind α_2 und c ringisomorph.

Hilfssatz 2. *Es sei $\mathfrak{R}'$ ein endlicher Ring, in dem der Grad jedes Elements eine Potenz einer Primzahl p ist. Wenn $\mathfrak{R}'$ zwei verschiedene Zerlegungen als direkte Summe unzerlegbarer Ideale besitzt, so ist die Anzahl der Faktoren gleich, und zu jedem Faktor der einen Zerlegung gibt es einen Faktor der anderen, der mit ihm ringisomorph ist.*

Beweis. Es seien

$$\mathfrak{R}' = \alpha_1 + \alpha_2 + \dots + \alpha_r = \beta_1 + \beta_2 + \dots + \beta_s$$

zwei Darstellungen von $\mathfrak{R}'$ als direkte Summe der unzerlegbaren Ideale. Da die Länge der Hauptkompositionsreihe von $\mathfrak{R}'$ eindeutig bestimmt ist⁽¹⁾, so ist der Satz in Analogie mit dem Beweise von O. Schmidt⁽²⁾ bewiesen, unter Anwendung vollständiger Induktion.

Die Gesamtheit aller Elemente b_i aus β_i ($i=1, 2, \dots, s$) von der Eigenschaft, dass $b_i \beta_i \equiv 0 \pmod{\alpha_k}$, bildet ein Ideal β'_i und ferner ist

$$\alpha_k \equiv 0 \pmod{\alpha'_k = \beta'_1 + \beta'_2 + \dots + \beta'_s},$$

denn für jedes Element a_k aus α_k wird $a_k = b_1 + b_2 + \dots + b_s$ und wegen $b_i \beta_i = a_k \beta_i \equiv 0 \pmod{\alpha_k}$ erhalten wir $b_i \equiv 0 \pmod{\beta'_i}$ ($i=1, 2, \dots, s$).

Setzen wir

$$\delta_k = [\alpha_1 + \dots + \alpha_{k-1} + \alpha_{k+1} + \dots + \alpha_r, \alpha'_k],$$

so werden $\alpha'_k = \alpha_k + \delta_k$, $\mathfrak{R}' \delta_k = (0)$, da $[\alpha_k, \delta_k] = (0)$ ist.

1. Fall. *Die erste Zerlegung enthält wenigstens zwei Faktoren, etwa α_1, α_2 , die beide nicht Totalnullteiler sind. Wenn $\mathfrak{R}' = \alpha'_1$ wäre,*

(1) M. Sono, On Congruences.

(2) O. Schmidt, Ueber unendliche Gruppen mit endlicher Kette, Math. Zeitschr. 29 (1929), S. 34-41.

so würden $\mathfrak{d}_1 = \alpha_2 + \dots + \alpha_r$, $\mathfrak{R}''(\alpha_2 + \dots + \alpha_r) = (0)$, $\mathfrak{R}''\alpha_2 = (0)$; was unmöglich ist. Somit soll $\alpha'_1 \neq \mathfrak{R}''$ sein, also ist α'_1 von kürzerer Kompositionsreihe als $\mathfrak{R}''$. Wir können daher für α'_1 den Satz voraussetzen, und wir erhalten

$$\alpha'_1 = \bar{b}'_1 + \bar{b}'_2 + \dots + \bar{b}'_s, \quad \alpha_1 \simeq \bar{b}'_1, \quad \bar{b}'_1 \equiv 0 \pmod{(\mathfrak{b}'_1)}.$$

Da $\alpha'_1 \neq (0)$ ist, so soll auch $\bar{b}'_1 \neq (0)$ sein. Wegen $\bar{b}'_1 \equiv 0 \pmod{(\alpha_1)}$ folgt $[\alpha_1, \bar{b}'_1] \neq (0)$, daraus folgt nach Zusatz $[\bar{b}'_1, \mathfrak{d}_1] = (0)$, da $\bar{b}'_1$ unzerlegbar ist.

Ferner wird $[\bar{b}'_1, \alpha_2 + \alpha_3 + \dots + \alpha_r] = (0)$, also folgt wegen der Endlichkeit von $\mathfrak{R}''$ sofort

$$\mathfrak{R}'' = \alpha_1 + \alpha_2 + \dots + \alpha_r = \bar{b}'_1 + \alpha_2 + \dots + \alpha_r = \mathfrak{b}_1 + \mathfrak{b}_2 + \dots + \mathfrak{b}_s$$

und $\bar{b}'_1 = \mathfrak{b}_1$ ist, da $\mathfrak{b}_1$ unzerlegbar ist, und $\bar{b}'_1 \equiv 0 \pmod{(\mathfrak{b}'_1)}$, $\mathfrak{b}'_1 \equiv 0 \pmod{(\mathfrak{b}_1)}$. Nach Hilfssatz 1 wird also

$$\alpha_2 + \dots + \alpha_r \simeq \mathfrak{b}_2 + \dots + \mathfrak{b}_s.$$

Seien nun $\bar{\alpha}_i$ ($i=2, 3, \dots, s$) die durch diesen Isomorphismus $\mathfrak{b}_i$ zugeordneten Ideale, dann wird

$$\alpha_2 + \alpha_3 + \dots + \alpha_r = \bar{\alpha}_2 + \bar{\alpha}_3 + \dots + \bar{\alpha}_s.$$

Da der Ring aber von kürzerer Kompositionsreihe als $\mathfrak{R}''$ ist, so werden

$$r = s, \quad \alpha_i \simeq \bar{\alpha}_i \simeq \mathfrak{b}_i \quad (i=2, 3, \dots, s).$$

2. Fall. α_1 ist der einzige Faktor, der nicht Totalnullteiler ist. Hätte die andere Zerlegung zwei verschiedene Faktoren $\mathfrak{b}_1, \mathfrak{b}_2$, die nicht Totalnullteiler sind, so würden wegen $\mathfrak{R}''\mathfrak{b}_k = \alpha_1\mathfrak{b}_k \neq (0)$, ($k=1, 2$)

$$[\alpha_1, \mathfrak{b}_1] \neq (0), \quad [\alpha_1, \mathfrak{b}_2] \neq (0)$$

im Widerspruch mit dem Zusatz. Es kann daher einen und nur einen Faktor $\mathfrak{b}_1$ in zweiter Zerlegung geben, der nicht Totalnullteiler ist, und ferner ist $\alpha_1\mathfrak{b}_1 \neq (0)$. Nach der Voraussetzung sind $\alpha_2, \dots, \alpha_r, \mathfrak{b}_2, \dots, \mathfrak{b}_s$ zyklische Gruppen, deren Grad eine Potenz der Primzahl p ist. Setzen wir

$$\mathfrak{R}'' = \alpha_1 + \alpha'_1 = \mathfrak{b}_1 + \mathfrak{b}'_1, \quad \alpha'_1 = \alpha_2 + \dots + \alpha_r, \quad \mathfrak{b}'_1 = \mathfrak{b}_2 + \dots + \mathfrak{b}_s,$$

so ist die Anzahl der verschiedenen Elemente aus α_1'' gleich der Anzahl der Elemente aus b_1'' , denn für zwei verschiedene Elemente α_1'' , $\bar{\alpha}_1''$ aus α_1'' werden wegen $[\alpha_1, b_1']=(0)$, $[\alpha_1'', b_1]=(0)$

$$\alpha_1'' = b_1 + b_1' , \quad \bar{\alpha}_1'' = \bar{b}_1 + \bar{b}_1' , \quad b_1' \neq \bar{b}_1'$$

und umgekehrt. Die p^a maligen Summen aller Elemente aus $\mathfrak{R}''$ bilden ein Ideal $\bar{\mathfrak{R}}''$, und wenn $\bar{\alpha}_1$, $\bar{\alpha}_1''$, $\bar{b}_1$, $\bar{b}_1''$ die α_1 , α_1'' , b_1 , b_1'' entsprechenden Ideale bedeuten, so werden auch

$$\bar{\mathfrak{R}}'' = \bar{\alpha}_1 + \bar{\alpha}_1'' = \bar{b}_1 + \bar{b}_1'' , \quad [\bar{\alpha}_1, \bar{b}_1']=(0) , \quad [\bar{\alpha}_1'', \bar{b}_1]=(0)$$

und die Grade der Gruppen (Ideale) $\bar{\alpha}_1''$ und $\bar{b}_1''$ sind gleich. Daraus folgt leicht⁽¹⁾, dass die Gruppen (Ideale) α_1'' , b_1'' dieselben Invarianten besitzen; also ist α_1'' mit b_1'' ringisomorph und $r=s$, $\alpha_i \simeq b_i$ ($i=2, 3, \dots, s$).

Mit Hilfe der Beziehung erhalten wir auch

$$\mathfrak{R}'' = \alpha_1 + \alpha_1'' = \alpha_1 + b_1'' = b_1 + b_1'' ,$$

weil $[\alpha_1, b_1']=(0)$ ist. Damit folgt auch nach Hilfssatz 1, dass α_1 mit b_1 ringisomorph ist.

3. Fall. *Alle Faktoren sind Totalnullteiler.* Der Satz ist in diesem Falle ganz klar.

Aus der im vorigen Paragraphen ausgesprochenen Tatsache und dem Hilfssatz ergibt sich endlich

Satz 17. *Die Darstellung von $\mathfrak{R}$ als direkte Summe der direkt unzerlegbaren Ringe ist bis auf Ringisomorphie eindeutig bestimmt.*

August 1930.

(1) Speiser, Die Theorie der Gruppen von endlicher Ordnung, 2. Aufl. §16.