Über primäre Ringe.

Von

Shinziro MORI.

(Eingegangen am 20. 4. 1935.)

Den Anstoss zu dieser Arbeit gaben die Note des Herrn W. Krull: „*Ein Satz über primäre Integritätsbereiche*",[1] und die Note des Herrn Y. Akizuki: „*Über die primären Integritätsbereiche mit Teilerkettensatz*".[2] In der vorliegenden Arbeit verstehen wir unter einem „*primären Ring* $\mathfrak{R}$" einen kommutativen Ring, in dem jedes Ideal (einschl. das Nullideal) stets primär ist, und in $\mathfrak{R}$ nehmen wir die Gültigkeit des Wohlordnungssatzes und folglich das folgende Lemma von Krull an[3]

Es sei S ein multiplikativ abgeschlossenes System aus dem Ring $\mathfrak{R}$, das kein Element aus dem Ideal $\mathfrak{a}$ enthält. Dann gibt es stets einen Primidealteiler $\mathfrak{p}$ von $\mathfrak{a}$, der zu S elementefremd ist und die Eigenschaft hat, dass in jedem echten Teiler von $\mathfrak{p}$ mindestens ein Element aus S vorkommt.

Bei dieser Definition behandle ich zuerst die Struktur des primären Ringes $\mathfrak{R}$, und dann die Eigenschaft des zu $\mathfrak{R}$ gehörigen ganz abgeschlossenen Ringes $\mathfrak{O}$. In dem besonderen Fall, wo in $\mathfrak{R}$ der eingeschränkte Vielfachenkettensatz gilt, $\mathfrak{R}$ das Einheitselement besitzt, und das Nullideal aus $\mathfrak{R}$ prim ist, zeige ich durch eine einfache Beweismethode die Gültigkeit des Satzes von Krull.

Über primäre Ringe, in denen das Lemma von Krull gilt.

Unter einem „*primären Ring* $\mathfrak{R}$" verstehen wir einen kommuta-

---

(1) W. Krull, Ein Satz über primäre Integritätsbereiche, Math. Annalen **103** (1930), 450–465.

(2) Der Umriss dieser Arbeit ist auf dem Kongress der „Physico-Mathematical Society of Japan," gehalten am 4. 4. 1935 an der Universität Osaka, verlesen worden.

(3) W. Krull, Idealtheorie in Ringen ohne Endlichkeitsbedingung, Math. Annalen **101** (1929), 732.

tiven Ring, in dem jedes Ideal (einschl. das Nullideal) immer primär ist.[1]

Ist ein Primideal $\mathfrak{p}$ aus $\mathfrak{R}$ vom Nullideal und von $\mathfrak{R}$ verschieden, so heisst $\mathfrak{p}$ „*echtes Primideal*".

Für die Struktur des primären Ringes gilt der folgende

Satz 1. *Ein primärer Ring $\mathfrak{R}$ ist ein Ring ohne echtes Primideal, oder ein Ring mit Einheitselement, der nur ein einziges echtes Primideal besitzt. Im letzten Fall ist das echte Primideal ein maximales Ideal.*

Zunächst seien $\mathfrak{p}_1$ und $\mathfrak{p}_2$ die verschiedenen echten Primideale aus $\mathfrak{R}$. Dann soll $\mathfrak{p}_1 \equiv 0\,(\mathfrak{p}_2)$, oder $\mathfrak{p}_2 \equiv 0\,(\mathfrak{p}_1)$ sein. Sonst würde $[\mathfrak{p}_1, \mathfrak{p}_2] = \mathfrak{d}$ kein Primärideal. Wir nehmen damit $\mathfrak{p}_1 \equiv 0\,(\mathfrak{p}_2)$ an. Da $\mathfrak{p}_1 \neq \mathfrak{p}_2$, $\mathfrak{p}_1 \neq (0)$ ist, so können wir ein durch $\mathfrak{p}_1$ unteilbares Element p_2 aus $\mathfrak{p}_2$ und ein von Null verschiedenes Element p_1 aus $\mathfrak{p}_1$ finden. Das Ideal (p_1p_2) ist nach unserer Voraussetzung auch ein Primärideal, und p_2 ist nicht-nilpotent in bezug auf (p_1p_2). Daher folgt, dass p_1 durch (p_1p_2) teilber sein muss; also wird

$$p_1 = p_1p_2', \qquad p_2' \equiv 0 \ (\mathfrak{p}_2)\,.$$

Für jedes durch $\mathfrak{p}_1$ unteilbare Element r aus $\mathfrak{R}$ gilt damit

$$p_1(r - rp_2') = 0\,, \qquad r - rp_2' \equiv 0 \ (\mathfrak{p}_1)\,.$$

Weil das Nullideal auch primär ist. Daraus folgt unmittelbar, dass jedes Element aus $\mathfrak{R}$ durch $(p_2', \mathfrak{p}_1)$, folglich durch $\mathfrak{p}_2$ teilbar sein muss. Das widerspricht unserer Voraussetzung, dass $\mathfrak{p}_2$ von $\mathfrak{R}$ verschieden ist. Damit muss $\mathfrak{p}_1 = (0)$ sein, wenn $\mathfrak{R} \neq \mathfrak{p}_2$ ist. Ist r ein durch $\mathfrak{p}_2$ unteilbares Element aus $\mathfrak{R}$, so erhalten wir auch.

$$p_2 \equiv 0 \ \big((rp_2)\big)\,, \qquad p_2 = r'p_2\,. \tag{1}$$

Da (0) prim ist, so soll das Element r' das Einheitselement aus $\mathfrak{R}$ sein.

Zweitens sei das Nullideal nicht prim, und $\mathfrak{p}_2$ ein einziges echtes Primideal. Dann folgt nach dem Lemma von Krull, dass jedes Element aus $\mathfrak{p}_2$ nilpotent ist. Aber nach (1) ergibt sich $p_2(r' - r'^2) = 0$, $r' - r'^2 \equiv 0\,(\mathfrak{p}_2)$, und dabei soll $r' \not\equiv 0\,(\mathfrak{p}_2)$ sein; sonst würde $p_2 = r'p_2 =$

---

(1) Das Wort „*Primärideal*" gebrauchen wir in Sinne von E. Noether. In der strengen Terminologie von Noether müssten wir von „*schwachen*" Primäridealen reden.

$r'^2 \mathfrak{p}_2 = \cdots\cdots = 0$. Für eine hinreichend grosse ganze Zahl m erhalten wir damit

$$(r' - r'^2)^m = 0\,, \qquad r'^m = r'^{2m} r''\,, \qquad r'^m r'' = (r'^m r'')^2\,,$$

wo r'' ein Element aus $\mathfrak{R}$ ist. Setzen wir $e = r'^m r''$, so wird $e = e^2 \not\equiv 0\ (\mathfrak{p}_2)$, und damit wird $e(r_1 - er_1) = 0$ für ein beliebiges Element r_1 aus $\mathfrak{R}$. Daher folgt, dass $\mathfrak{R}$ ein Ring mit Einheitselement und einem einzigen echten Primideal ist.

Ist das einzige echte Primideal $\mathfrak{p}_2$ durch ein von $\mathfrak{R}$ verschiedenes Ideal $\mathfrak{a}$ teilbar, so ist $\mathfrak{a}$ kein Primideal. Das zugehörige Halbprimideal $\mathfrak{h}$ von $\mathfrak{a}$ ist auch primär, und folglich muss $\mathfrak{h} = \mathfrak{R}$ sein; was unmöglich ist, da $\mathfrak{R}$ das Einheitselement besitzt. Damit soll $\mathfrak{R} = \mathfrak{a}$ sein.

Satz 2. *Der durch $\mathfrak{R}$ bestimmte Quotientenring $\mathfrak{K}$ ist dann und nur dann von $\mathfrak{R}$ verschieden,*[1] *wenn $\mathfrak{R}$ ein echtes Ideal besitzt, und wenn das Nullideal prim ist.*

Nach dem Satz 1 können wir die folgenden drei Fälle unterscheiden.

Zuerst besitze $\mathfrak{R}$ kein echtes Primideal. Besitzt $\mathfrak{R}$ kein Einheitselement, so ist nach dem Lemma von Krull jedes Element von $\mathfrak{R}$ nilpotent in bezug auf ein beliebiges vom Nullideal verschiedenes Ideal oder das Nullideal, je nachdem das Nullideal von $\mathfrak{R}$ prim ist oder nicht. Im ersten Fall ist $\mathfrak{R} \neq \mathfrak{K}$, und im zweiten Fall existiert der Quotientenring nicht. Besitzt $\mathfrak{R}$ das Einheitselement, so ist $\mathfrak{R}$ ein Körper und folglich wird $\mathfrak{R} = \mathfrak{K}$.

Zweitens besitze $\mathfrak{R}$ ein echtes Primideal $\mathfrak{p}$, und sei das Nullideal aus $\mathfrak{R}$ nicht prim. Dann ist jedes Element aus $\mathfrak{p}$ nilpotent, und für beliebige durch $\mathfrak{p}$ unteilbare Flemente r, r' ist $r \equiv 0\,\big((r')\big)$. Denn nach Satz 1 besitzt $\mathfrak{R}$ das Einheitselement e, und es ist $e \equiv r'r''\ (\mathfrak{p})$, $e = r'r'' + p$. Aus $p^k = 0$ für eine hinreichend grosse Zahl k folgt damit $e = r'r'''$. Also ist $\mathfrak{R} = \mathfrak{K}$.

Drittens besitze $\mathfrak{R}$ ein echtes Primideal $\mathfrak{p}$, und sei das Nullideal prim. Ist r ein durch $\mathfrak{p}$ unteilbares Element aus $\mathfrak{R}$ und p ein von Null verschiedenes Element aus $\mathfrak{p}$, so ist $\dfrac{r}{p}$ ein Element aus $\mathfrak{K}$, aber kein Element aus $\mathfrak{R}$.

Nach dem Satz 2 sollen wir für unsere Untersuchungen vom zu $\mathfrak{R}$

(1) Der Quotientenring $\mathfrak{K}$ ist der Ring aller Brüche $\dfrac{a}{b}$, wo a, b die Elemente aus $\mathfrak{R}$ sind, und b kein Nullteiler ist, mit den üblichen Rechnungsregeln. Vgl. H. Grell, Beziehungen zwischen den Idealen verschiedener Ringe, Math. Annalen **97** (1927), 499.

gehörigen ganz abgeschlossenen Ring annehmen,[1] dass der primäre Ring $\mathfrak{R}$ ein echtes Ideal, aber keinen Nullteiler besitzt. Im folgenden bedeutet damit der primäre Ring $\mathfrak{R}$ stets einen kommutativen Ring mit Einheitselement und einem einzigen echten Primideal $\mathfrak{p}$, aber ohne Nullteiler, oder einen Ring ohne Nullteiler, in denen jedes Element nilpotent in bezug auf ein beliebiges Ideal $\left(\neq (0)\right)$ ist. Folglich ist der durch $\mathfrak{R}$ bestimmte Quotientenring $\mathfrak{K}$ ein Körper, und der zu $\mathfrak{R}$ gehörige ganz abgeschlossene Ring $\mathfrak{O}$ ist ein Ring ohne Nullteiler.

Satz 3. *Es sei $\mathfrak{O}$ ein zu $\mathfrak{R}$ gehöriger ganz abgeschlossener Ring. Besitzt ein vom Nullideal verschiedenes Ideal $\mathfrak{a}_0$ aus $\mathfrak{O}$ einen echten Teiler $\mathfrak{b}_0$, und ist ein Element aus $\mathfrak{b}_0$ nicht nilpotent in bezug auf $\mathfrak{a}_0$, so gibt es in $\mathfrak{b}_0$ ein idempotentes Element in bezug auf $\mathfrak{a}_0$.*

Besitzt $\mathfrak{R}$ kein Einheitselement, so ist jedes Element aus $\mathfrak{R}$ nilpotent in bezug auf ein beliebiges Ideal $\left(\neq (0)\right)$. Aus der Gleichung $\alpha^n + a_1\alpha^{n+1} + \dots + a_n = 0$ mit den Koeffizienten a_i aus $\mathfrak{R}$ folgt damit, dass jedes Element α aus $\mathfrak{O}$ auch nilpotent in bezug auf jedes Ideal

(1) Die Gesamtheit $\mathfrak{O}$ aller Elemente α aus $\mathfrak{K}$, denen eine Gleichung $\alpha^n + a_1\alpha^{n-1} + \dots + a_n = 0$ mit den Koeffizienten a_i aus $\mathfrak{R}$ genügen, heisst der „*zu $\mathfrak{R}$ gehörige ganz abgeschlossene Ring.*"

Besitzt $\mathfrak{R}$ kein Einheitselement und keinen Nullteiler, so ist die Gesamtheit $\mathfrak{O}$ aller Elemente α aus $\mathfrak{K}$, denen eine Gleichung $\alpha^n + a_1\alpha^{n-1} + \dots + a_n = 0$ mit den Koeffizienten a_i aus $\mathfrak{R}$ genügen, auch ein Ring. Denn, wenn $f(\beta) = \beta^m + b_1\beta^{m-1} + \dots + b_m = 0$ ist, so setzen wir $\beta = \omega + \alpha$, so erhalten wir $\alpha^m + \frac{1}{(m-1)!} f^{(m-1)}(\omega)\alpha^{m-1} + \dots + f(\omega) = 0$. Eliminieren wir α, so ergibt sich

$$\begin{array}{r} m \text{ Zeilen} \left\{ \begin{array}{c} \\ \\ \\ \\ \end{array} \right. \\ n \text{ Zeilen} \left\{ \begin{array}{c} \\ \\ \\ \\ \end{array} \right. \end{array} \left| \begin{array}{cccccccc} \varepsilon & a_1 & a_2 & \dots & a_n & & & \\ & \varepsilon & a_1 & \dots & \dots & a_n & & \\ & & \dots & \dots & \dots & \dots & & \\ & & & \varepsilon & a_1 & \dots & \dots & a_n \\ \varepsilon & \frac{1}{(m-1)!} f^{(m-1)}(\omega) & \dots & f'(\omega) & f(\omega) & & & \\ & \varepsilon & & \dots & & f(\omega) & & \\ & & & \dots & \dots & \dots & & \\ & & & \varepsilon & \dots & \dots & \dots & f(\omega) \end{array} \right| = 0,$$

wo ε das Einheitselement aus $\mathfrak{K}$ bedeutet. Nach der Entwicklung von Laplace erhalten wir daraus $\omega^{mn} + c_1\omega^{mn-1} + \dots + c_{mn} = 0$, wo c die Elemente aus $\mathfrak{R}$ sind. Also gehört $\omega = \beta - \alpha$ auch zu $\mathfrak{O}$. In gleicher Weise können wir leicht zeigen, dass $\alpha\beta$ auch zu $\mathfrak{O}$ gehört, und dass θ zu $\mathfrak{O}$ gehört, wenn θ eine Gleichung $\theta^k + \alpha_1\theta^{k-1} + \dots + \alpha_k = 0$ mit den Koeffizienten α aus $\mathfrak{O}$ genügt. Vgl. P. Bachmann, *Allgemeine Arithmetik der Zahlenkörper*, S. 6.

$(\neq (0))$ aus $\mathfrak{O}$ ist. Somit können wir uns auf den Ring $\mathfrak{R}$ mit Einheitselement beschränken.

Ist $\mathfrak{b}_0 = \mathfrak{O}$, so ist unsere Behauptung schon einleuchtend, da $\mathfrak{R}$ das Einheitselement e besitzt. Hiermit nehmen wir $\mathfrak{O} \neq \mathfrak{b}_0$ an. Es sei β ein durch $\mathfrak{a}_0$ unteilbares Element aus $\mathfrak{b}_0$, und nicht nilpotent in bezug auf $\mathfrak{a}_0$. In der Gleichung mit den Koeffizienten a_i aus $\mathfrak{R}$

$$\beta^n + a_1\beta^{n+1} + \ldots\ldots + a_{n-1}\beta + a_n = 0$$

soll $a_n \equiv 0\,(\mathfrak{p})$ sein. Sonst würde $e \equiv 0\,(\mathfrak{b}_0)$, und folglich hätten wir einen Widerspruch $\mathfrak{O} = \mathfrak{b}_0$. Da $\mathfrak{a}_0 \neq (0)$ ist, so enthält $\mathfrak{a}_0$ ein von Null verschiedenes Element p' aus $\mathfrak{p}$. Wären alle Koeffizienten a_i durch $\mathfrak{p}$ teilbar, so würde $\beta^{nm} \equiv 0\,(\mathfrak{a}_0)$ für eine hinreichend grosse ganze Zahl m. Das ist aber nach unserer Voraussetzung unmöglich. Damit wird

$$a_n \equiv 0\,, \quad a_{n-1} \equiv 0\,, \quad \ldots\ldots, \quad a_{i+1} \equiv 0\,(\mathfrak{p})\,, \quad a_i \not\equiv 0\,(\mathfrak{p}) \quad (1 \leqq i < n)\,,$$

und für eine grosse ganze Zahl k

$$(\beta^n + a_1\beta^{n-1} + \ldots\ldots + a_i\beta^{n-i})^k \equiv 0 \;\; (\mathfrak{a}_0)\,.$$

Aus $a_i^k a' = e - p,\;\; p \equiv 0\,(\mathfrak{p})$ folgt

$$a_i^k a'(e + p + p^2 + \ldots\ldots + p^s) \equiv e\,(\mathfrak{a}_0)\,,$$

oder

$$a_i^k a'' \equiv e\,(\mathfrak{a}_0)\,, \qquad a'' \equiv 0\,(\mathfrak{R})\,.$$

Daher erhalten wir

$$\beta^{k(n-i)} + a_1'\beta^{k(n-i)+1} + \ldots\ldots \equiv 0 \;\; (\mathfrak{a}_0)\,,$$

wo die Koeffizienten die Elemente aus $\mathfrak{R}$ sind. Folglich wird $\beta^{k(n-i)} \equiv \beta^{2k(n-i)}\beta'\,(\mathfrak{a}_0)$. Setzen wir $\varepsilon = \beta^{k(n-i)}\beta'$, so folgt daher

$$\varepsilon \equiv \varepsilon^2 \;\; (\mathfrak{a}_0)\,, \qquad \varepsilon \not\equiv 0 \;\; (\mathfrak{a}_0)\,, \qquad \varepsilon \equiv 0 \;\; (\mathfrak{b}_0)\,.$$

Aus Satz 3 folgt unmittelbar folgender

Satz 4. *Jedes echte Primideal aus $\mathfrak{O}$ ist ein maximales Ideal von $\mathfrak{O}$.*

Satz 5. *Jedes Ideal aus $\mathfrak{O}$ ist als Durchschnitt von endlich oder unendlich vielen Primäridealen darstellbar.*

Besitzt $\mathfrak{R}$ kein Einheitselement, so ist jedes Ideal aus $\mathfrak{O}$ primär. Damit nehmen wir an, dass $\mathfrak{R}$ das Einheitselement und ein einziges echtes Primideal $\mathfrak{p}$ besitzt. Wir können jedem Element $a\;(\neq 0)$ der wohlgeordneten Menge $\mathfrak{R}$ das Element $\alpha = \frac{a}{p^s}$ mit der grössten Potenz s, für die $\frac{a}{p^s}$ ein Element aus $\mathfrak{O}$ ist, zuordnen. Sind $\alpha' = \frac{a}{p^k}$, $\frac{\alpha'}{p} = \frac{a}{p^{k+1}}$ beide die Elemente aus $\mathfrak{O}$, so soll $a \equiv 0\,(\mathfrak{p})$, $\alpha' \equiv 0\,(\mathfrak{p}\mathfrak{O})$ sein. Damit genügt jedem durch $\mathfrak{p}\mathfrak{O}$ unteilbaren Element β aus $\mathfrak{O}$ eine Kongruenz $\beta \equiv \frac{b}{p^t}\,(\mathfrak{p}\mathfrak{O})$ und dabei ist $\frac{b}{p^{t+1}}$ kein Element aus $\mathfrak{O}$. Also ist $\mathfrak{O}\,|\,\mathfrak{p}\mathfrak{O}$ einer Teilmenge von $\mathfrak{R}$ äquivalent.

Andererseits ist das zugehörige Halbprimideal $\mathfrak{h}_0$ eines Ideals $\dot{\mathfrak{a}}_0\,(\neq (0))$ aus $\mathfrak{O}$ ein Teiler von $\mathfrak{p}\mathfrak{O}$. Hiermit ist die Menge $\mathfrak{O}\,|\,\mathfrak{h}_0$ einer Teilmenge von $\mathfrak{R}$ äquivalent, und folglich gilt in $\mathfrak{O}\,|\,\mathfrak{h}_0$ der Wohlordnungssatz. Nach dem Lemma von Krull ist damit $\mathfrak{h}_0$ durch ein echtes Primideal teilbar. Also ist $\mathfrak{a}_0$ durch ein echtes Primideal teilbar, und nach dem Satz 4 folgt unser Satz.[1]

Über primäre Ringe mit Vielfachenkettensatz.

In diesem Paragraphen verstehen wir unter $\mathfrak{R}$ einen primären Ring, der dem eingeschränkten Vielfachenkettensatz genügt,[2] mit dem Quotientenring $\mathfrak{K}$ und dem zugehörigen ganz abgeschlossenen Ring $\mathfrak{O}$.

Satz 6. *In $\mathfrak{O}$ gilt auch der eingeschränkte Vielfachenkettensatz.*

---

(1) W. Krull, Idealtheorie in Ringen ohne Endlichkeitsbedingung, Math. Annalen, **101** (1929), 738.

(2) Wenn $\mathfrak{R}$ ein echtes Primideal besitzt, und wenn in $\mathfrak{R}$ der eingeschränkte Vielfachenkettensatz gilt, so gilt der Teilerkettensatz auch in $\mathfrak{R}$. Denn für ein von Null verschiedenes nicht-primes Ideal $\mathfrak{a}$ ist $\mathfrak{a}_1 = \mathfrak{a} : \mathfrak{p}$ ein echter Teiler von $\mathfrak{a}$, und $\mathfrak{a}_2 = \mathfrak{a}_1 : \mathfrak{p}$ ist auch ein echter Teiler von $\mathfrak{a}_1$, und so weiter. Daher erhalten wir $\mathfrak{a} : \mathfrak{a}_1 > \mathfrak{a} : \mathfrak{a}_2 > \mathfrak{a} : \mathfrak{a}_3 > \ldots$, weil $\mathfrak{p}^2\mathfrak{a}_2 \equiv 0\,(\mathfrak{a})$, $\mathfrak{p}^2\mathfrak{a}_3 \not\equiv 0\,(\mathfrak{a})$ ist. Nach dem Vielfachenkettensatz erhalten wir damit $\mathfrak{p}^n \equiv 0\,(\mathfrak{a})$ für eine ganze Zahl n. Andererseits gilt $\mathfrak{p} = (p_1, p_2, \ldots, p_m, \mathfrak{p}^2)$, und daher folgt der Teilerkettensatz.

Wenn $\mathfrak{R}$ kein echtes Primideal, aber Nullteiler besitzt, so folgt aus dem eingeschränkten Vielfachenkettensatz nicht der Teilerkettensatz. Vgl. S. Mori, Über eindeutige Reduktion von Idealen in Ringen ohne Teilerkettensatz, dieses Journal **3** (1933), 188.

Besitzt $\mathfrak{R}$ keinen Nullteiler und kein echtes Primideal, so gilt auch der Teilerkettensatz. Ist p ein von Null verschiedenes Element aus $\mathfrak{R}$, so soll nach dem Vielfachenkettensatz das Produkt hinreichend vieler Elemente stets durch (p) teilbar sein, und daher folgt $\mathfrak{R}^n \equiv 0\,((p))$ für eine grosse ganze Zahl n. Weiter besitzt $\mathfrak{a} = (p) : \mathfrak{R}$ eine endliche Basis und daraus folgt die Gültigkeit des Teilerkettensatzes.

Zum Beweise genügt es, nur den Ring $\mathfrak{R}$ mit einem echten Ideal $\mathfrak{p}$ und ohne Nullteiler zu betrachten. Es sei $\mathfrak{a}_0$ ein vom Nullideal verschiedenes Ideal aus $\mathfrak{O}$. Dann können wir in $\mathfrak{a}_0$ ein nicht-verschwindendes Element p aus $\mathfrak{p}$ finden, und jedes Element aus $\mathfrak{O}$ ist in der Form $\frac{a}{p^s}$ darstellbar, wo a ein Element aus $\mathfrak{R}$ bedeutet. Es sei $\mathfrak{a}_1$ die Gesamtheit aller Elemente a_i aus $\mathfrak{R}$ von der Art, dass $\frac{a_i}{p}$ ein Element aus $\mathfrak{O}$ ist. Dann ist $\mathfrak{a}_1$ offenbar ein Ideal aus $\mathfrak{R}$. Wenn wir $\mathfrak{a}_2$ in gleicher Weise definieren, so ist $\mathfrak{a}_1$ ein Teiler von $\mathfrak{a}_2$. In solcher Weise erhalten wir eine Vielfachenkette der Ideale aus $\mathfrak{R}$

$$\mathfrak{a}_1 \geqq \mathfrak{a}_2 \geqq \mathfrak{a}_3 \geqq \ldots\ldots$$

Betrachten wir daraus die Vielfachenkette der Ideale aus $\mathfrak{R}$

$$\big((p)\mathfrak{R}, \mathfrak{a}_1\big) \geqq \big((p)\mathfrak{R}, \mathfrak{a}_2\big) \geqq \ldots\ldots \geqq (p)\mathfrak{R},$$

so muss die Kette nach dem eingeschränkten Vielfachenkettensatz im Endlichen abbrechen, und wir erhalten

$$\big((p)\mathfrak{R}, \mathfrak{a}_{n-1}\big) \neq \big((p)\mathfrak{R}, \mathfrak{a}_n\big) = \big((p)\mathfrak{R}, \mathfrak{a}_{n+1}\big) = \ldots\ldots \tag{1}$$

Ist $\alpha = \frac{a}{p^s}$ $(s \geqq n)$ ein durch $\mathfrak{a}_0$ unteilbares Element aus $\mathfrak{O}$, so wird $a \equiv 0\ (\mathfrak{a}_s)$ und aus (1) folgt

$$a = bp + a_{s+1}, \qquad a_{s+1} \equiv 0\ \ (\mathfrak{a}_{s+1}), \qquad b \equiv 0\ \ (\mathfrak{R}).$$

Da $\frac{a}{p^s}$, $\frac{a_{s+1}}{p^{s+1}}$ die Elemente aus $\mathfrak{O}$ sind, so erhalten wir(1)

$$\frac{a_{s+1}}{p^s} \equiv 0\ \ (\mathfrak{a}_0), \qquad \alpha \equiv \frac{b}{p^{s-1}}\ \ (\mathfrak{a}_0).$$

Hiermit gilt für jedes durch $\mathfrak{a}_0$ unteilbare Element α

$$\alpha \equiv \frac{r}{p^m}\ \ (\mathfrak{a}_0) \qquad (m < n), \qquad r \equiv 0\ \ (\mathfrak{R}).$$

Existiert in $\mathfrak{O}$ eine unendliche Vielfachenkette der Ideale aus $\mathfrak{O}$

$$\mathfrak{a}_0^{(1)} \supset \mathfrak{a}_0^{(2)} \supset \mathfrak{a}_0^{(3)} \supset \ldots\ldots \supset \mathfrak{a}_0,$$

(1) Diese Beweismethode stammt von Herrn Y. Akizuki.

so können wir in $\mathfrak{O}$ unendlich viele Elemente α_i finden, so dass $\alpha_i \equiv 0\,(\mathfrak{a}_0^{(i)})$, $\alpha_i \not\equiv 0\,(\mathfrak{a}_0^{(i+1)})$ ist. Aber nach dem soeben gewonnenen Ergebnis können wir $\alpha_i \equiv \frac{r_i}{p^{s_i}}\,(\mathfrak{a}_0)$ $(s_i < n)$ $(i = 1, 2, \ldots.)$ setzen. Damit soll für unendlich viele $\alpha_{m_j} \equiv \frac{r_{m_j}}{p^{s_{m_j}}}\,(\mathfrak{a}_0)$ $(m_1 < m_2 < m_3 < \ldots.)$

$$s_{m_1} = s_{m_2} = s_{m_3} = \ldots. < n$$

sein. Nun bilden wir die folgenden Ideale aus $\mathfrak{R}$

$$\mathfrak{a}_{m_1} = (r_{m_1}, r_{m_2}, r_{m_3}, \ldots., p^n), \qquad \mathfrak{a}_{m_2} = (r_{m_2}, r_{m_3}, \ldots., p^n),$$

$$\mathfrak{a}_{m_3} = (r_{m_3}, \ldots., p^n), \qquad \ldots\ldots\ldots\ldots$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

Wäre $\mathfrak{a}_{m_1} = \mathfrak{a}_{m_2}$, so würde

$$r_{m_1} = (z_2 + c_2)r_{m_2} + (z_3 + c_3)r_{m_3} + \ldots. + (z + c)p^n,$$

dabei dedeuten c die Elemente aus $\mathfrak{R}$, und z die ganzen rationalen Zahlen. Durch Division mit $p^{s_{m_1}}$ hätten wir

$$\alpha_{m_1} \equiv (z_2 + c_2)\alpha_{m_2} + (z_3 + c_3)\alpha_{m_3} + \ldots.\,(\mathfrak{a}_0).$$

Also würde $\alpha_{m_1} \equiv 0\,(\mathfrak{a}_0^{(m_2)})$ und ein Widerspruch ergäbe sich. Daher folgt die Existenz einer unendlichen Vielfachenkette der Ideale aus $\mathfrak{R}$

$$\mathfrak{a}_{m_1} \supset \mathfrak{a}_{m_2} \supset \mathfrak{a}_{m_3} \supset \ldots. \supset (p^n).$$

Das ist nach dem eingeschränkten Vielfachenkettensatz im Ring $\mathfrak{R}$ unmöglich. Damit soll in $\mathfrak{O}$ der eingeschränkte Vielfachenkettensatz gelten.

Satz 7 (Satz von Krull). *Es sei das Nullideal aus $\mathfrak{R}$ prim, und $\mathfrak{R}$ besitze das Einheitselement. Dann lässt jedes Ideal aus $\mathfrak{O}$ sich als Produkt von Potenzen endlich vieler fester, paarweise teilerfremder Primideale darstellen.*

Wegen Satz 2 können wir uns auf den Ring $\mathfrak{R}$ mit dem einzigen echten Primideal $\mathfrak{p}$ beschränken. Es sei ein vom Nullideal verschiedenes Ideal $\mathfrak{a}_0$ nicht primär, und es sei $\mathfrak{h}_0$ das zugehörige Halbprimideal von $\mathfrak{a}_0$. Dann ist $\mathfrak{h}_0$ nicht prim, und nach den Sätzen 3 und 6 wird

$\mathfrak{O} \mid \mathfrak{h}_0 = (\varepsilon_1) + (\varepsilon_2) + \ldots\ldots + (\varepsilon_m)$, wo ε_i die idempotenten Elemente in bezug auf $\mathfrak{h}_0$ sind. Ferner ist $\mathfrak{p}_0^{(i)} = (\varepsilon_1, \ldots\ldots \varepsilon_{i-1}, \varepsilon_{i+1}, \ldots\ldots, \varepsilon_m, \mathfrak{h}_0)$ ein Primideal, und wir erhalten $\mathfrak{a}_0 = [\mathfrak{q}_0^{(1)}, \ldots\ldots, \mathfrak{q}_0^{(m)}]$, wo $\mathfrak{q}_0^{(i)}$ ein zu $\mathfrak{p}_0^{(i)}$ gehöriges Primärideal ist.

Es sei $\mathfrak{p}_0$ ein echtes Primideal aus $\mathfrak{O}$, und es sei $\mathfrak{p}_0^{-1} = \mathfrak{O} : \mathfrak{p}_0$ die Gesamtheit der Elemente π aus $\mathfrak{K}$ von der Art, dass $\pi\mathfrak{p}_0$ in $\mathfrak{O}$ enthalten ist.(1) Dann ist $\mathfrak{p}_0^{-1}$ ein gebrochenes Ideal aus $\mathfrak{O}$. Ist $p \equiv 0\ (\mathfrak{p}_0)$, $(p) \neq (0)$, $(p) \neq \mathfrak{p}_0$, so können wir ein Element p' in $\mathfrak{p}_0$ finden, so dass $p' \not\equiv 0\ \big((p)\big)$, $p'\mathfrak{p}_0 \equiv 0\ \big((p)\big)$ ist. Damit enthält $\mathfrak{p}_0^{-1}$ ein wirklich-gebrochenes Element $\dfrac{p'}{p}$. Nach dem Vielfachenkettensatz folgt aus der Struktur von $\mathfrak{O}|(p)$, dass $\mathfrak{p}_0$ eine endliche Basis besitzt, und daher wird $\mathfrak{p}_0\mathfrak{p}_0^{-1} = \mathfrak{O}$, da $\mathfrak{p}_0$ ein maximales Ideal ist. Ist $\mathfrak{q}_0 \equiv 0\ (\mathfrak{p}_0)$, $\mathfrak{p}_0^2 \equiv 0\ (\mathfrak{q}_0)$, so soll $\mathfrak{p}_0^{-1}\mathfrak{q}_0 = \mathfrak{p}_0$, oder $\mathfrak{p}_0^{-1}\mathfrak{q}_0 = \mathfrak{O}$ sein. Damit gibt es kein Ideal zwischen $\mathfrak{p}_0$ und $\mathfrak{p}_0^2$, und daher folgt, dass ein zu $\mathfrak{p}_0$ gehöriges Primärideal $\mathfrak{q}_0$ einer Potenz von $\mathfrak{p}_0$ gleich ist.(2) Da jedes echte Primideal aber nach Satz 4 maximal ist, so folgt unmittelbar der Satz von Krull.

Ist $\mathfrak{R}$ ohne Nullteiler und besitzt kein Einheitselement, so ist nach dem Beweis von Satz 3 jedes vom Nullideal verschiedene Ideal aus $\mathfrak{O}$ primär. Betrachten wir einen primären Ring $\mathfrak{R}$ ohne Nullteiler und Einheitselement, so müssen wir damit den Satz von Krull in folgender Weise umformen.

Es sei $\mathfrak{R}$ ein primärer Ring mit Vielfachenkettensatz, und es sei $\mathfrak{O}$ der zu $\mathfrak{R}$ gehörige ganz abgeschlossene Ring. Dann ist jedes Ideal aus $\mathfrak{O}$ als kürzester Durchschnitt der zu verschiedenen Primidealen gehörigen Primärideale eindeutig darstellbar.

(1) Vgl. B. L. van der Waerden, Zur Produktzerlegung der Ideale in ganz-abgeschlossenen Ringen, Math. Annalen **101** (1929), 298.

(2) M. Sono, On Congruences II, Memoirs of the College of Science, Kyoto Imperial University **3** (1918), 123.