Einige Eigenschaften primärer Integritätsbereiche.

Von

Shinziro MORI.

(Eingegangen am 20. 9. 1935.)

Mit Hilfe der Bewertungstheorie hat W. Krull[1] einen bemerkenswerten Satz über die Zerlegung der Ideale vom Ring $\mathfrak{J}^*$ bewiesen, der zu einem primären Integritätsbereich $\mathfrak{J}$ mit Teilerkettensatz gehört, und ganz abgeschlossen ist. In dieser Schrift werde ich auf die speziellen Eigenschaften des zu $\mathfrak{J}$ gehörigen ganz abgeschlossenen Ringes $\mathfrak{J}^*$ vom Standpunkt der Gleichung, der die Elemente von $\mathfrak{J}^*$ genügen, weiter eingehen.

Über das minimale Radikal in $\mathfrak{J}^*$.

Unter dem *primären Integritätsbereich $\mathfrak{J}$ mit dem Teilerkettensatz* verstehen wir einen Ring mit Einheitselement, aber ohne echte Nullteiler, in dem jedes Ideal primär ist und der Teilerkettensatz gilt. Dann ist $\mathfrak{J}$ ein Körper, oder ein Integritätsbereich mit einem einzigen Primideal $\mathfrak{p}\left(\neq(0)\right)$.[2] Im ersten Fall spielt $\mathfrak{J}$ aber doch eine ganz untergeordnete Rolle. Von vornherein betrachten wir damit nur den zweiten Fall. Das einzige Primideal $\mathfrak{p}$ besitzt folglich die Eigenschaft:

$\mathfrak{p}$ ist stets nilpotent in bezug auf jedes Ideal $\left(\neq(0)\right)$, das durch $\mathfrak{p}$ teilbar ist.

Ferner können wir leicht beweisen, dass *aus der Voraussetzung*

(1) W. Krull, Ein Satz über primäre Integritätsbereiche, Math. Annalen **103** (1930), 450–465. W. Krull, *Idealtheorie*, § 4, § 5. Y. Akizuki, Einige Bemerkungen über primäre Integritätsbereiche mit Teilerkettensatz, Proc. Phys.—Math. Soc. Japan **17** (1935), 327.

(2) Vgl. S. Mori, Über primäre Ringe, Dieses Journal **5** (1935), 132.

des Teilerkettensatzes in $\mathfrak{J}$ *auch die Gültigkeit des eingeschränkten Vielfachenkettensatzes folgt.*[1]

Es sei $\mathfrak{R}$ der Quotientenkörper von $\mathfrak{J}$. Genügt ein Element α aus $\mathfrak{R}$ einer Gleichung $\alpha^n + a_1\alpha^{n-1} + \ldots + a_n = 0$ mit Koeffizienten aus $\mathfrak{J}$, so nennen wir das Element α *ganz abhängig von* $\mathfrak{J}$. Die Gesamtheit $\mathfrak{J}^*$ aller von $\mathfrak{J}$ ganz abhängigen Elemente aus $\mathfrak{R}$ ist ein Ring, und ferner sind alle von $\mathfrak{J}^*$ ganz abhängigen Elemente auch in $\mathfrak{J}^*$ selbst enthalten. Also ist $\mathfrak{J}^*$ ein ganz abgeschlossener Ring. Wir nennen hiermit $\mathfrak{J}^*$ den *zu* $\mathfrak{J}$ *gehörigen ganz abgeschlossenen Ring.*

Im Folgenden bezeichnen wir immer die Ideale aus $\mathfrak{J}$ mit deutschen Buchstaben und die Ideale aus $\mathfrak{J}^*$ mit deutschen Buchstaben mit einem Stern. Die griechischen Buchstaben bezeichnen stets die Elemente aus $\mathfrak{J}^*$, oder aus $\mathfrak{R}$, und die lateinischen Buchstaben die Elemente aus $\mathfrak{J}$, und ferner bezeichnen wir mit $a, b, \ldots, p$ die Elemente aus $\mathfrak{p}$ und mit $r, \ldots$ die durch $\mathfrak{p}$ unteilbaren Elemente aus $\mathfrak{J}$.

Bekanntlich ist das *Radikal eines Ideals* $\mathfrak{a}^*$ *aus* $\mathfrak{J}^*$ das Ideal aller der Elemente aus $\mathfrak{J}^*$, von denen eine Potenz zu $\mathfrak{a}^*$ gehört. Ist das Radikal $\mathfrak{r}^*$ eines Ideals $\mathfrak{a}^*$ $\left(\neq (0)\right)$ aus $\mathfrak{J}^*$ in jedem vom Null verschiedenen Radikal aus $\mathfrak{J}^*$ enthalten, so soll $\mathfrak{r}^*$ das *minimale Radikal in* $\mathfrak{J}^*$ heissen.

Satz 1. *Genügt ein Element* α *aus* $\mathfrak{R}$ *einer Gleichung* $\alpha^n + a_1\alpha^{n-1} + \ldots + a_n = 0$ *mit den Koeffizienten* a_i *aus* $\mathfrak{p}$, *so ist die Gesamtheit* $\mathfrak{r}^*$ *aller dieser Elemente* α *das minimale Radikal in* $\mathfrak{J}^*$.

Es sei p ein von Null verschiedenes Element aus $\mathfrak{p}$. Dann ist $\mathfrak{a}^* = p\mathfrak{J}^*$ ein Ideal aus $\mathfrak{J}^*$, und jedes Element aus $\mathfrak{r}^*$ ist nilpotent in bezug auf $\mathfrak{a}^*$. Ist ein Element α' aus $\mathfrak{J}^*$ nilpotent in bezug auf $\mathfrak{a}^*$, so soll

$$\alpha'^k = p \cdot \gamma, \qquad \gamma^m + c_1\gamma^{m-1} + \ldots + c_m = 0, \qquad c_i \equiv 0 \ (\mathfrak{J})$$

sein. Daraus folgt unmittelbar

$$\alpha'^{km} + c_1 p\alpha'^{k(m-1)} + \ldots + c_m p^m = 0,$$

dabei sind die Koeffizienten Elemente aus $\mathfrak{p}$. Hiermit muss α' auch zu

(1) Ist $\mathfrak{a}\left(\neq (0)\right)$ ein von $\mathfrak{J}$ verschiedenes Ideal aus $\mathfrak{J}$, so muss $\mathfrak{a}$ durch $\mathfrak{p}$ teilbar sein. Da $\mathfrak{p}$ nilpotent in bezug auf $\mathfrak{a}$ ist, so können wir ein Ideal $\mathfrak{a}'$ zwischen $\mathfrak{a}$ und einem beliebigen Teiler $\mathfrak{a}_1$ von $\mathfrak{a}$ finden, so dass es kein Ideal zwischen $\mathfrak{a}$ und $\mathfrak{a}'$ gibt, und daher folgt die Gültigkeit des eingeschränkten Vielfachenkettensatzes.

$\mathfrak{r}^*$ gehören; also ist $\mathfrak{r}^*$ das Radikal von $\mathfrak{a}^*$. Da p aber ein beliebiges Element aus $\mathfrak{p}$ ist, so soll $\mathfrak{r}^*$ das minimale Radikal in $\mathfrak{J}^*$ sein.

Satz 2. *Es sei α ein Element aus $\mathfrak{J}^*$, und k sei der niederste Grad der Gleichung, der α genügt. α gehört dann und nur dann nicht zum minimalen Radikal $\mathfrak{r}^*$ in $\mathfrak{J}^*$, wenn α irgendeiner Gleichung*

$$\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-i-1}\alpha^{i+1} + r\alpha^i + \ldots + a_n = 0, \qquad n \geqq k > i \geqq 0$$

mit Koeffizienten aus $\mathfrak{J}$ genügt, wo r ein durch $\mathfrak{p}$ unteilbares Element bedeutet.

Gehört α nicht zu $\mathfrak{r}^*$, so genügt α nach Satz 1 keiner Gleichung, deren gesamte Koeffizienten bis auf den ersten Elemente aus $\mathfrak{p}$ sind. Folglich erfüllt die Gleichung vom niedersten Grad, der α genügt, die im Satz ausgesprochene Bedingung.

Jetzt nehmen wir die Gültigkeit der Gleichung

$$(1)\quad f(\alpha) = \alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-i-1}\alpha^{i+1} + r\alpha^i + \ldots + a_n = 0,$$

$$n \geqq k > i \geqq 0, \qquad r \not\equiv 0 \ (\mathfrak{p})$$

mit Koeffizienten aus $\mathfrak{J}$ an. Dann werden wir beweisen, dass α keiner Gleichung

$$(2)\qquad \varphi(\alpha) = \alpha^m + b_1\alpha^{m-1} + \ldots + b_m = 0, \qquad m \geqq k$$

genügt, dabei sind alle b_i Elemente aus $\mathfrak{p}$. Zu diesem Zweck werden wir die Gültigkeit von (2) annehmen und zwei verschiedene Fälle unterscheiden.

1. Fall. Es sei $m \leqq n$. Dann folgt aus (1) und (2)

$$(3)\quad \varphi_1(\alpha) = f(\alpha) - \alpha^{n-m}\varphi(\alpha)$$

$$= c_1\alpha^{n-1} + c_2\alpha^{n-2} + \ldots + c_{n-i-1}\alpha^{i+1} + r_1\alpha^i + \ldots + c_n = 0$$

$$0 \leqq i < k \leqq m \leqq n, \qquad r_1 \not\equiv 0 \ (\mathfrak{p}).$$

Ist $c_1 \equiv 0 \ (\mathfrak{p})$, so folgt aus (1) und (3)

$$(4)\quad \varphi_2(\alpha) = c_1 f(\alpha) - \alpha\varphi_1(\alpha)$$

$$= d_1\alpha^{n-1} + \ldots + d_{n-i-2}\alpha^{i+2} + r_2\alpha^{i+1} + \ldots + d_n = 0,$$

$$r_2 \not\equiv 0 \ (\mathfrak{p}).$$

Indem wir so fortfahren, erhalten wir endlich

$$(5) \qquad \varphi_{n-i}(\alpha) = r_{n-i}\alpha^{n-1} + \ldots + k_n = 0, \qquad r_{n-i} \not\equiv 0 \ (\mathfrak{p}).$$

Da für ein passendes Element r' aus $\mathfrak{J}$ $r_{n-i}r' = 1 - p^s p'$ ist, so wird $1 = r_{n-i}r' + p^s p'$, dabei ist s eine hinreichend grosse ganze Zahl und p ein beliebig bestimmtes Element aus $\mathfrak{p}$. Durch Multiplikation mit r' erhalten wir aus (5)[1]

$$(6) \qquad \varphi'_{n-i}(\alpha) = \alpha^{n-1} + l_2\alpha^{n-2} + \ldots + l_n = 0.$$

Sind alle l_i durch $\mathfrak{p}$ teilbar, so bilden wir die Summe von (3) und (6)

$$\varphi_1(\alpha) + \varphi'_{n-1}(\alpha)$$
$$= (c_1+1)\alpha^{n-1} + (c_2+l_2)\alpha^{n-2} + \ldots + (r_1+l_{n-i})\alpha^i + \ldots + c_n + l_n = 0.$$

Dann sind die Koeffizienten c_1+1 und r_1+l_{n-i} beide durch $\mathfrak{p}$ unteilbar. Durch Multiplikation mit einem passend bestimmten Element r'' erhalten wir

$$\alpha^{n-1} + t_2\alpha^{n-2} + \ldots + \bar{r}\alpha^i + \ldots + t_n = 0$$
$$0 \leqq i < k \leqq m \leqq n, \qquad \bar{r} \not\equiv 0 \ (\mathfrak{p}).$$

Ist (1) die Gleichung vom niedersten Grad, die die vorher erwähnte Eigenschaft besitzt, so ergibt sich ein Widerspruch.

2. Fall. Es sei, $m > n$. Teilen wir $\varphi(\alpha)$ durch $f(\alpha)$, so ergibt sich

$$\varphi(\alpha) = f(\alpha)q(\alpha) + r(\alpha)$$
$$r(\alpha) = p_0\alpha^{n-1} + p_1\alpha^{n-2} + \ldots + p_{n-1} = 0,$$
$$q(\alpha) = \alpha^{m-n} + q_1\alpha^{m-n-1} + \ldots + q_{m-n}.$$

Nach der obigen Beweismethode müssen alle Koeffizienten p_i durch $\mathfrak{p}$ teilbar sein, wenn (1) die Gleichung vom niedersten Grad ist, die die im Satz ausgesprochene Eigenschaft besitzt. Es seien durch $\mathfrak{p}$ $a_n, a_{n-1}, \ldots, a_{s+1}$ teilbar, aber a_s unteilbar, und es seien durch $\mathfrak{p}$ $q_{m-n}, q_{m-n-1}, \ldots, q_{t+1}$ teilbar, aber q_t unteilbar. Dann ist der Koeffizient von $\alpha^{m-t-s}(s \geqq 1)$

$$a_s q_t + a_{s-1}q_{t+1} + \ldots + a_{s+1}q_{t-1} + \ldots \equiv 0 \ (\mathfrak{p}),$$

(1) $a = \frac{a}{p}$, dabei ist p ein Element aus $\mathfrak{p}$.

und daraus folgt unmittelbar $a_s q_t \equiv 0(\mathfrak{p})$; das ist aber unmöglich. Die Annahme der Gültigkeit von (2) also ist falsch, wenn (1) die Gleichung vom niedersten Grad ist, die die oben erwähnte Eigenschaft hat.

Im allgemeinen können wir ganz genau wie bei den obigen Fällen unter Anwendung vollständiger Induktion die Ungültigkeit von (2) beweisen. Folglich soll α nicht zu $\mathfrak{r}^*$ gehören.

Eine Folge der Beweismethode dieses Satzes ist:

Zusatz. *Es seien* $\alpha^k + a_1\alpha^{k-1} + \ldots + a_k = 0$, $\alpha^k + a_1'\alpha^{k-1} + \ldots + a_k' = 0$ *zwei Gleichungen vom niedersten Grad* k, *den* α *genügt. Dann soll* $a_i \equiv a_i'$ $(\mathfrak{p})$ $(i = 1, 2, \ldots, k)$ *sein.*

Nun wollen wir mit Hilfe der früheren Sätze den folgenden Satz beweisen.

Satz 3. $\mathfrak{p}$ *ist dann und nur dann das minimale Radikal in* $\mathfrak{J}^*$, *wenn jedes Element* α *aus* $\mathfrak{J}^*$ *stets irgendeiner Gleichung*

$$\alpha^n + r_1\alpha^{n_1} + r_2\alpha^{n_2} + \ldots + r_{s-1}\alpha^{n_{s-1}} + r_s\alpha + p_1 = 0\,,$$

$$n > n_1 > n_2 > \ldots n_{s-1} > 1\,,$$

$$r_i \not\equiv 0 \ (\mathfrak{p}) \qquad (i = 1, \ldots, s), \qquad r_0 = 1\,, \qquad p_1 \equiv 0 \ (\mathfrak{p})$$

mit Koeffizienten aus $\mathfrak{J}$ *genügt.*

Zunächst sei $\mathfrak{p}$ das minimale Radikal in $\mathfrak{J}^*$, und α sei ein Element aus $\mathfrak{J}^*$, das nicht zu $\mathfrak{J}$ gehört. Dann gehört α nicht zum minimalen Radikal in $\mathfrak{J}^*$, und folglich soll α nach Satz 2 einer Gleichung

$$(1) \qquad \alpha^m + \ldots + r\alpha^i + a_{m-i+1}\alpha^{i-1} + \ldots + a_m = 0\,,$$

$$r \not\equiv 0 \ (\mathfrak{p})\,, \qquad a_m, a_{m-1}, \ldots, a_{m-i+1} \equiv 0 \ (\mathfrak{p}) \qquad 0 \leqq i < m$$

mit Koeffizienten aus $\mathfrak{J}$ genügen. Ist b ein beliebiges Element aus $\mathfrak{p}$, so muss stets $\alpha^m b \equiv 0$ $(\mathfrak{p})$ für jede ganze Zahl m sein. Hiermit folgt aus (1)

$$\alpha^m + r_1\alpha^{m_1} + \ldots + r_{s-1}\alpha^{m_{s-1}} + r_s\alpha^i \equiv 0 \ (\mathfrak{p})\,,$$

$$m > m_1 > \ldots > m_{s-1} > i \geqq 0\,, \qquad r_j \not\equiv 0 \ (\mathfrak{p}) \qquad (j = 1, 2, \ldots, s).$$

Da $\mathfrak{p}$ aber das Radikal ist, so folgt aus $\alpha^i(\alpha^{m-i} + r_1\alpha^{m_1-i} + \ldots + r_{s-1}\alpha^{m_{s-1}-i} + r_s) \equiv 0$ $(\mathfrak{p})$

$$\alpha(\alpha^{m-i} + r_1\alpha^{m_1-i} + \ldots + r_s) + p_1 = 0\,.$$

Also ist $\alpha^n + r_1\alpha^{n_1} + \ldots + r_{s-1}\alpha^{n_{s-1}} + r_s\alpha + p_1 = 0$, $n > n_1 > \ldots > n_{s-1} > 1$.

Ist α ein Element aus $\mathfrak{J}$, so wird $\alpha+p_1=0$, $p_1\equiv 0$ $(\mathfrak{p})$, oder $\alpha^2+\alpha r_1=0$ $r_1\not\equiv 0$ $(\mathfrak{p})$, je nachdem α zu $\mathfrak{p}$ gehört oder nicht. Damit ist die Bedingung notwendig.

Umgekehrt nehmen wir die Gültigkeit der Bedingung an, und es sei α ein beliebiges Element aus $\mathfrak{J}^*$. Gehört α nicht zu $\mathfrak{J}$, so ist der niederste Grad der Gleichung, der α genügt, nicht kleiner als 2. Nach Satz 2 folgt damit, dass α keiner Gleichung von der Form $\alpha^m+a_1\alpha^{m-1}+\ldots.+a_m=0$, $a_i\equiv 0$ $(\mathfrak{p})$ genügt. Ist $\mathfrak{r}^*$ das minimale Radikal in $\mathfrak{J}^*$, so gehört α damit nicht zu $\mathfrak{r}^*$. Mit anderen Worten gehört α nicht zu $\mathfrak{r}^*$, wenn α kein Element von $\mathfrak{J}$ ist. Also soll $\mathfrak{p}$ mit $\mathfrak{r}^*$ identisch sein.

Endlich fügen wir noch einen leicht beweisbaren Satz an:

Satz 4. *Ist* $\mathfrak{r}^*$ *das minimale Radikal in* $\mathfrak{J}^*$, *und ist*

$$\mathfrak{J}^*\supset\mathfrak{r}_1^*\supset\mathfrak{r}_2^*\supset\ldots.\supset\mathfrak{r}_l^*=\mathfrak{r}^*$$

eine Hauptreihe der Ideale aus $\mathfrak{J}^*$, *so ist die Länge* l *gleich der Anzahl aller voneinander verschiedenen Primideale* $(\not\equiv(0),\not\equiv\mathfrak{J}^*)$ *von* $\mathfrak{J}^*$.

Struktur der speziellen primären Integritätsbereiche.

Satz 5. $\mathfrak{J}$ *ist dann und nur dann mit* $\mathfrak{J}^*$ *identisch, wenn* $\mathfrak{p}$ *in* $\mathfrak{J}$ *ein Hauptideal ist.*[1]

Zunächst nehmen wir an, dass $\mathfrak{p}=(p)$ ist. Ist α ein beliebiges Element aus $\mathfrak{J}^*$, so wird

$$\alpha^n+a_1\alpha^{n-1}+\ldots.+a_n=0\,,\qquad \alpha=\frac{a}{p^s}\,,$$

wobei alle a_i die Elemente aus $\mathfrak{J}$ bedeuten. Wenn $s\geqq 1$ ist, so muss a zu $\mathfrak{p}$ gehören. Aber aus $\mathfrak{p}=(p)$ folgt $a=pa'$, und daher erhalten wir $\alpha=\frac{a'}{p^{s-1}}$. In solcher Weise erhalten wir endlich $\alpha=a^{(s)}$. Folglich soll $\mathfrak{J}^*=\mathfrak{J}$ sein.

Zweitens nehmen wir an, dass $\mathfrak{J}^*=\mathfrak{J}$ ist. Nach dem Teilerkettensatz existiert ein Hauptideal (p) von der Art, dass (p) durch $\mathfrak{p}$ teilbar, aber durch jedes andere Hauptideal ausser (1) unteilbar ist.

(1) Dieser Satz ist bekannt. Hier wollen wir einen elementaren Beweis geben.

Ist ein Element p' durch (p) unteilbar und $p'^m = pp''$, so soll $p'' \equiv 0$ $(\mathfrak{p})$ sein. Sonst würde für ein passendes Element r

$$rp'^m = p(1-d), \qquad d \equiv 0 \left((p'^m)\right).$$

Folglich hätten wir $p \equiv 0\left((p'^m)\right)$; also ergäbe sich ein Widerspruch, dass das Hauptideal (p') aus $\mathfrak{p}$ ein echter Teiler von (p) wäre. Wir können $(p) \subset (p, p') \subset \ldots. \subset (p, p', \ldots., p^{(s)}) = \mathfrak{p}$ setzen, und dabei folgt aus der Eigenschaft von $\mathfrak{p}$ $(p^{(i)})^{k_i} \equiv 0(p)$ $(i = 1, 2, \ldots., s)$. Setzen wir damit $N = k_1 + k_2 + \ldots. + k_s$, so ist die N-te Potenz jedes Elementes aus $\mathfrak{p}$ stets durch p teilbar. Hiermit besitzt ein Element p_1 aus $\mathfrak{p}$ den grössten Exponenten n, für welchen $p_1^{n-1} \not\equiv 0(p)$, $p_1^n \equiv 0(p)$ ist. Hier nehmen wir $n \geqq 2$ an, d. h. dass $\mathfrak{p}$ kein Hauptideal ist. Aus $p_1^n \equiv 0$ (p), $p \not\equiv 0(p_1^n)$ folgt

$$p_1^n = pp_2, \qquad p_2 \equiv 0 \ (\mathfrak{p}). \tag{1}$$

Wäre $p_2^{n-1} \equiv 0((p, p_1^{n-1}))$, so würde $p_2^{n-1} = ap + a_1 p_1^{n-1}$. Durch Multiplikation mit p^{n-1} hätten wir nach (1)

$$p_1^{n(n-1)} = ap^n + a_1 p_1^{n-1} p^{n-1}, \qquad \text{oder} \qquad \left(\frac{p_1^{n-1}}{p}\right)^n = a + a_1 \frac{p_1^{n-1}}{p},$$

wobei $\dfrac{p_1^{n-1}}{p}$ kein Element aus $\mathfrak{J}$ wäre. Damit ergäbe sich ein Widerspruch $\mathfrak{J} \neq \mathfrak{J}^*$. Damit soll $p_2^{n-1} \not\equiv 0((p, p_1^{n-1}))$ sein. Da n der grösste Exponent in bezug auf (p) ist, so wird auch

$$p_2^n = pp_3, \qquad p_3 \equiv 0 \ (\mathfrak{p}). \tag{2}$$

Wäre $p_3^{n-1} \equiv 0((p, p_1^{n-1}, p_2^{n-1}))$, so würde $p_3^{n-1} = ap + a_1 p_1^{n-1} + a_2 p_2^{n-1}$. Durch Multiplikation mit $p^{(n+1)(n-1)}$ hätten wir nach (1) und (2)

$$p^{n^2(n-1)} = ap^{n^2} + a_1 p_1^{n-1} p^{n^2-1} + a_2 p^{n(n-1)} p_1^{n(n-1)},$$

oder

$$\left(\frac{p_1^{n-1}}{p}\right)^{n^2} = a + a_1 \frac{p_1^{n-1}}{p} + a_2 \left(\frac{p_1^{n-1}}{p}\right)^n.$$

Also hätten wir einen Widerspruch $\mathfrak{J} \neq \mathfrak{J}^*$. Damit muss $p_3^{n-1} \not\equiv 0((p, p_1^{n-1}, p_2^{n-1}))$ sein. Im allgemeinen sei

$$p_k^n = pp_{k+1}, \qquad p_{k+1} \equiv 0 \ (\mathfrak{p}). \tag{3}$$

Dann muss $p_{k+1}^{n-1} \not\equiv 0((p, p_1^{n-1}, p_2^{n-1}, \ldots., p_k^{n-1}))$ sein. Wäre

$$p_{k+1}^{n-1} = ap + a_1 p_1^{n-1} + \ldots + a_k p_k^{n-1},$$

so hätten wir durch Multiplikation mit p^{n^k-1} aus (1), (2) und (3)

$$p_1^{n^k(n-1)} = ap^{n^k} + a_1 p_1^{n-1} p^{n^k-1} + a_2 p_1^{n(n-1)} p^{n(n^k-1-1)} + \ldots.$$
$$+ a_k p_1^{n^{k-1}(n-1)} p^{n^{k-1}(n-1)}.$$

Daraus folgte $\left(\frac{p_1^{n-1}}{p}\right)^{n^k} = a + a_1 \frac{p_1^{n-1}}{p} + a_2 \left(\frac{p_1^{n-1}}{p}\right)^n + \ldots. + a_k \left(\frac{p_1^{n-1}}{p}\right)^{n^{k-1}}$;
also ergäbe sich ein Widerspruch gegen $\mathfrak{J} = \mathfrak{J}^*$. In solcher Weise erhalten wir endlich eine unendliche Kette von Idealen $(p) \subset (p, p_1^{n-1}) \subset (p, p_1^{n-1}, p_2^{n-1}) \subset \ldots.$ Aber jede Teilerkette muss im Endlichen abbrechen, und daher folgt auch ein Widerspruch. Damit ist die Annahme $n \geqq 2$ falsch, und unser Satz ist in allen seinen Teilen vollständig bewiesen.

Satz 6. *Es sei* $\mathfrak{J} \neq \mathfrak{J}^*$, *und es sei* p *ein in* $\mathfrak{p}$ *unzerlegbares Element*(1) *aus* $\mathfrak{p}$ *und* $\mathfrak{q} = (p) : \mathfrak{p}$ *der Idealquotient in* $\mathfrak{J}$. $\mathfrak{p}$ *ist dann und nur dann der Führer*(2) *von* $\mathfrak{J}$ *hinsichtlich* $\mathfrak{J}^*$, *wenn* $\mathfrak{J}^*$ *identisch mit der Gesamtheit* $\mathfrak{g}$ *der Elemente* $\frac{q}{p}$ *ist, dabei läuft* q *alle Elemente von* $\mathfrak{q}$ *durch.*

Nach Satz 5 ist $\mathfrak{p}$ kein Hauptideal in $\mathfrak{J}$, und folglich ist der Idealquotient $\mathfrak{q} = (p) : \mathfrak{p}$ ein durch $\mathfrak{p}$ teilbares Ideal in $\mathfrak{J}$.

Nach der Voraussetzung, dase $\mathfrak{p}$ der Führer von $\mathfrak{J}$ ist, ist

$$(1) \qquad (p')\mathfrak{J}^* \subseteqq \mathfrak{J}$$

für jedes Element p' aus $\mathfrak{p}$. Andererseits ist das in $\mathfrak{J}$ nicht enthaltende Element α aus $\mathfrak{J}^*$ in der Form $\alpha = \frac{q}{p^s}$, $q \not\equiv 0 \ (p)$, $q \equiv 0 \ (\mathfrak{p})$ darstellbar. Aus (1) soll damit $s = 1$, und

$$(2) \qquad \alpha = \frac{q}{p}, \qquad q \not\equiv 0 \ (p), \qquad q \equiv 0 \ (\mathfrak{q})$$

---

(1) Ist p_0 ein in $\mathfrak{p}$ zerlegbares Element aus $\mathfrak{p}$, und ist $p_0 = p_1 \cdot p_1'$, so wird $(p_0) < (p_1)$ unter Berücksichtigung der Bedingung, dass es in $\mathfrak{J}$ keinen Nullteiler gibt. Sind p_1 und p_1' beide noch zerlegbar in $\mathfrak{p}$ und ist $p_1 = p_2 \cdot p_2'$, so wird $(p_0) < (p_1) < (p_2)$. Nach dem Teilerkettensatz sollen wir endlich ein in $\mathfrak{p}$ unzerlegbares Element p erhalten.

(2) Unter dem *Führer von* $\mathfrak{J}$ *hinsichtlich* $\mathfrak{J}^*$ verstehen wir das grösste Ideal aus $\mathfrak{J}^*$, das eine Untermenge von $\mathfrak{J}$ ist.

sein. Und zwar sollen alle Elemente α aus $\mathfrak{J}^*$ in $\mathfrak{g}$ enthalten sein. Es sei umgekehrt α ein durch (2) definiertes Element im Quotientenkörper $\mathfrak{R}$. Dann folgt aus $\mathfrak{q} = (p) : \mathfrak{p}$ leicht $q^2 = pp_1$. Wäre $p_1 \not\equiv 0(\mathfrak{p})$, so würde p zerlegbar[1] in $\mathfrak{J}$. Hiermit soll

$$q^2 = pp_1, \qquad p_1 \equiv 0 \ (\mathfrak{p}) \tag{3}$$

sein, und wir können zwei verschiedene Fälle unterscheiden.

I. Es sei $p_1 \equiv 0 \ (p)$. Dann wird $\left(\frac{q}{p}\right)^2 = p_2$, und folglich ist α ein Element aus $\mathfrak{J}^*$.

II. Es sei $p_1 \not\equiv 0 \ (p)$. Durch Multiplikation mit q ergibt sich aus (3)

$$q^3 = pp_1q = p^2p_2, \qquad p_2 \equiv 0 \ (\mathfrak{p}).$$

Denn, wäre $p_2 \not\equiv 0(\mathfrak{p})$, so würde p auch zerlegbar in $\mathfrak{p}$. Damit ist $p_2 \equiv 0(\mathfrak{p})$. Im Fall $p_2 \equiv 0(p)$ ist $\frac{q}{p} \subset \mathfrak{J}^*$, und im anderen Fall betrachten wir wieder

$$q^4 = p^3p_3, \qquad p_3 \equiv 0 \ (\mathfrak{p}).$$

Ist $p_3 \not\equiv 0(p)$, so wenden wir dieselbe Betrachtungsweise auf $q^4 = p^3p_3$ an. Indem wir diesen Prozess fortführen, wird $\frac{q}{p}$ ein Element von $\mathfrak{J}^*$, oder wir erhalten die Elemente $p_1, p_2, p_3 \ldots$. aus $\mathfrak{p}$, die alle durch p unteilbar sind, und

$$q^{i+1} = p^ip_i \qquad (i = 1, 2, \ldots.). \tag{4}$$

Aber nach dem Teilerkettensatz ergibt sich daraus

$$p_k \equiv r_1p_1 + r_2p_2 + \ldots. + r_{k-1}p_{k-1} \qquad ((p)),$$

wo r die Elemente aus $\mathfrak{J}$ sind. Aus (4) folgt damit

$$q^{k+1} \equiv r_1q^2p^{k-1} + r_2q^3p^{k-2} + \ldots. + r_{k-1}q^kp \qquad ((p^{k+1})),$$

oder
$$\left(\frac{q}{p}\right)^{k+1} = r_1\left(\frac{q}{p}\right)^2 + r_2\left(\frac{q}{p}\right)^3 + \ldots. + r_{k-1}\left(\frac{q}{p}\right)^k + r_0.$$

---

(1) Wäre $p_1 \not\equiv 0(\mathfrak{p})$, so würde für ein passendes Element r' aus $\mathfrak{J}$ $p_1r' = 1 - q^2q'$. Damit hätten wir $q^2r' = p(1 - q^2q')$, $p = q(qr' + pqq')$. Dabei wäre $q \equiv 0 \ (\mathfrak{p})$, $qr' + pqq' \equiv 0 \ (\mathfrak{p})$.

Also soll $\frac{q}{p}$ zu $\mathfrak{J}^*$ gehören. Zusammenfassend erhalten wir $\mathfrak{g} = \mathfrak{J}^*$.

Wir setzen umgekehrt voraus, es sei $\mathfrak{g} = \mathfrak{J}^*$. Ist $\alpha = \frac{q}{p}$ ein Element aus $\mathfrak{J}^*$, und ist p' ein beliebiges Element aus $\mathfrak{p}$, so wird $\alpha \cdot p' = \frac{q}{p} p' \subset \mathfrak{J}$, da $(q)\mathfrak{p} \equiv 0$ $((p))$ ist. Dabei soll ferner $\frac{qp'}{p} \subset \mathfrak{p}$ sein; sonst würde p zerlegbar in $\mathfrak{p}$. Hiermit ist $\mathfrak{p}$ ein Ideal in $\mathfrak{J}^*$, welches nur Elemente aus $\mathfrak{J}$ enthält. Wäre der Führer $\mathfrak{f}^*$ von $\mathfrak{J}$ hinsichtlich $\mathfrak{J}^*$ ein echter Teiler von $\mathfrak{p}$, so enthielte $\mathfrak{f}^*$ ein durch $\mathfrak{p}$ unteilbares Element aus $\mathfrak{J}$, und folglich würde $\mathfrak{J}^* = \mathfrak{f}^*$. Das ist nach $\mathfrak{J} \neq \mathfrak{J}^*$ unmöglich. Also muss $\mathfrak{f}^* = \mathfrak{p}$ sein.

Satz 7. *Das minimale Radikal* $\mathfrak{r}^*$ *in* $\mathfrak{J}^*$ *ist dann und nur dann prim, wenn jedes durch* $\mathfrak{r}^*$ *unteilbare Element* α *aus* $\mathfrak{J}^*$ *stets einer Gleichung*

$$\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha + r = 0, \qquad r \not\equiv 0 \ (\mathfrak{p})$$

genügt.

Sind $\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha + r = 0, \qquad r \not\equiv 0 \ (\mathfrak{p})$

$$\beta^m + b_1\beta^{m-1} + \ldots + b_{m-1}\beta + r' = 0, \qquad r' \not\equiv 0 \ (\mathfrak{p}),$$

und setzen wir $\omega = \alpha\beta$, so erhalten wir durch Elimination von α und β

$$\left.\begin{array}{l} m \text{ Zeilen} \\ \\ \\ \\ n \text{ Zeilen} \\ \\ \\ \end{array}\right\{ \left|\begin{array}{cccccccccc} 1 & a_1 & \ldots & a_{n-1} & r & 0 & \ldots & 0 \\ 0 & 1 & a_1 & \ldots & a_{n-1} & r & \ldots & 0 \\ \ldots & & & & & & & \\ 0 & & 1 & a_1 & \ldots & & a_{n-1} & r \\ r' & \omega b_{m-1} & \ldots & \omega^{m-1}b_1 & \omega^m & 0 & \ldots & 0 \\ 0 & r' & \ldots & & \omega^m & \ldots & 0 & \\ & & & \ldots & & & & \\ & & & r' & \omega b_{m-1} & \ldots & \omega^m & \end{array}\right| = 0$$

Daraus folgt $\omega^{mn} + c_1\omega^{mn-1} + \ldots + c_{mn-1}\omega + r^m r'^n = 0$, $r^m r'^n \not\equiv 0(\mathfrak{p})$. Nach Satz 2 gehört ω nicht zu $\mathfrak{r}^*$. Die Bedingung ist damit hinreichend.

Ist γ kein Element aus $\mathfrak{r}^*$, und genügt γ keiner Gleichung von der Gestalt $\gamma^n + a_1\gamma^{n-1} + \ldots + a_{n-1}\gamma + r = 0$, $r \not\equiv 0(\mathfrak{p})$, so soll γ einer Gleichung

$$\gamma^k + c_1\gamma^{k-1} + \ldots + r_{k-i}\gamma^i + c_{k-i+1}\gamma^{i-1} + \ldots + c_k = 0\,.$$

$$0 < i < k\,, \qquad c_{k-i+1} \equiv 0\ (\mathfrak{p}) \ldots c_k \equiv 0\ (\mathfrak{p})\,, \qquad r_{k-i} \not\equiv 0\ (\mathfrak{p})$$

genügen. Daher folgt $\gamma^i(\gamma^{k-i} + c_1\gamma^{k-i-1} + \ldots + r_{k-i}) \equiv 0(\mathfrak{r}^*)$, und dabei ist $\gamma^i \not\equiv 0(\mathfrak{r}^*)$. Wäre $\gamma^{k-i} + c_1\gamma^{k-i-1} + \ldots + r_{k-i} \equiv 0(\mathfrak{r}^*)$, so würde

$$(\gamma^{k-i} + \ldots + r_{k-i})^s + d_1(\gamma^{k-i} + \ldots + r_{k-i})^{s-1} + \ldots$$

$$+ d_{s-1}(\gamma^{k-i} + \ldots + r_{k-i}) + d_s = 0\,,$$

wo alle d durch $\mathfrak{p}$ teilbar sind. Daraus ergäbe sich ein Widerspruch, dass γ einer Gleichung $\gamma^{s(k-i)} + t_1\gamma^{s(k-i)-1} + \ldots + r_0 = 0$, $r_0 \not\equiv 0(\mathfrak{p})$ genügt. Hiermit soll $\gamma^{k-i} + c_1\gamma^{k-i-1} + \ldots + r_{k-1} \not\equiv 0(\mathfrak{r}^*)$ sein, und folglich ist $\mathfrak{r}^*$ nicht prim. Unsere Bedingung ist damit notwendig.

Aus den Sätzen 3 und 7 ziehen wir die bemerkenswerte Folgerung:

Satz 8. *$\mathfrak{p}$ ist dann und nur dann auch ein Primideal aus $\mathfrak{J}^*$, wenn alle nicht in $\mathfrak{p}$ enthaltenen Elemente a aus $\mathfrak{J}^*$ irgendeiner der folgenden Gleichungen*

$$a^n + a_1a^{n-1} + \ldots + a_{n-1}a + r_n = 0\,, \qquad r_n \not\equiv 0\ (\mathfrak{p})$$

genügen.

Über Einheiten.

Satz 9. *Ist ε ein Element aus $\mathfrak{J}^*$, so ist die Gültigkeit der Gleichung $\varepsilon^n + a_1\varepsilon^{n-1} + \ldots + a_{n-1}\varepsilon + a_n = 0$, $a_n \not\equiv 0\ (\mathfrak{p})$ die notwendige und hinreichende Bedingung dafür, dass auch $\frac{1}{\varepsilon}$ zu $\mathfrak{J}^*$ gehört.*[1]

Ist $a_n \not\equiv 0\ (\mathfrak{p})$ in der Gleichung $\varepsilon^n + a_1\varepsilon^{n-1} + \ldots + a_n = 0$, so gehört ε nicht zu $\mathfrak{p}$. Daraus folgt $a_n\left(\frac{1}{\varepsilon}\right)^n + a_{n-1}\left(\frac{1}{\varepsilon}\right)^{n-1} + \ldots + a_1\left(\frac{1}{\varepsilon}\right) + 1 = 0$, und für ein passendes Element r ist $a_n r = 1 + p^t q$, $\left(\frac{1}{\varepsilon}\right)^n p^t q \subset \mathfrak{p}$, dabei ist p ein von Null verschiedenes Element aus $\mathfrak{p}$ und t eine hinreichend grosse ganze Zahl. Daraus ergibt sich

(1) Ist ein Element r aus $\mathfrak{J}$ durch $\mathfrak{p}$ unteilbar, so wird $r\left(\frac{1}{r}\right) = 1$, und für ein passendes Element r' ist $rr' = 1 - (rp)q$, $p \equiv 0(\mathfrak{p})$. Damit ist $\frac{1}{r} = r' + pq$; also ist r eine Einheit.

$$\left(\frac{1}{\varepsilon}\right)^n + b_1\left(\frac{1}{\varepsilon}\right)^{n-1} + \ldots\ldots + b_{n-1}\left(\frac{1}{\varepsilon}\right) + b_n = 0\,, \qquad b_n \not\equiv 0\ (\mathfrak{p})\,.$$

Also gehört $\frac{1}{\varepsilon}$ auch zu $\mathfrak{J}^*$.

Es sei umgekehrt $\frac{1}{\varepsilon}$ auch ein Element von $\mathfrak{J}^*$. Dann wird

$$(1)\quad \left(\frac{1}{\varepsilon}\right)^n + b_1\left(\frac{1}{\varepsilon}\right)^{n-1} + \ldots\ldots + b_i\left(\frac{1}{\varepsilon}\right)^{n-i} + \ldots\ldots + b_n = 0\,.$$

Wären alle b durch $\mathfrak{p}$ teilbar, so folgte der Widerspruch $\mathfrak{r}^* = \mathfrak{J}^*$. Wir nehmen damit $b_{i+1}, b_{i+2}, \ldots\ldots, b_n \equiv 0(\mathfrak{p})$, $b_i \not\equiv 0(\mathfrak{p})$, $1 \leqq i \leqq n$ an. Dann folgt aus (1)

$$b_i\varepsilon^i + b_{i-1}\varepsilon^{i-1} + \ldots\ldots + b_1\varepsilon + 1 \equiv 0\ (\mathfrak{r}^*)\,, \qquad b_i \not\equiv 0\ (\mathfrak{p})\,,$$

oder
$$\varepsilon^i + b'_{i-1}\varepsilon^{i-1} + \ldots\ldots + b'_1\varepsilon + b' \equiv 0\ (\mathfrak{r}^*)\,, \qquad b' \not\equiv 0\ (\mathfrak{p})\,.$$

Nach Satz 1 folgt daraus

$$(\varepsilon^i + b'_{i-1}\varepsilon^{i-1} + \ldots\ldots + b')^k + c_1(\varepsilon^i + \ldots\ldots + b')^{k-1} + \ldots\ldots + c_{k-1}(\varepsilon^i + \ldots\ldots + b') + c_k = 0\,,$$

wo alle c durch $\mathfrak{p}$ teilbar sind. Durch Umformung der Gleichung erhalten wir $\varepsilon^{ik} + d_1\varepsilon^{ik-1} + \ldots\ldots + d_{ik-1}\varepsilon + d_{ik} = 0$, $d_{ik} \not\equiv 0(\mathfrak{p})$, und unser Satz ist bewiesen.

Ein Element ε aus $\mathfrak{J}^*$ heisst eine *Einheit*, wenn auch $\frac{1}{\varepsilon}$ zu $\mathfrak{J}^*$ gehört.

Aus Satz 9 folgt nun sogleich:

Satz 10. *Jedes Produkt von Einheiten ist auch eine Einheit.*

Satz 11. *Jedes Element α aus $\mathfrak{J}^*$ ist als Summe von Einheiten darstellbar, wenn $\mathfrak{J} \mid \mathfrak{p}$ ein Körper von der Charakteristik von 0 ist.*[1]

Zum Beweis sei

$$\alpha^n + a_1\alpha^{n-1} + \ldots\ldots + r\alpha^i + a_{n-i+1}\alpha^{i-1} + \ldots\ldots + a_n = 0\,,$$

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

und wir setzen $\alpha = \alpha' + x$, $x \not\equiv 0\ (\mathfrak{p})$, dabei ist x ein Element aus $\mathfrak{J}$. Dann wird

(1) E. Steinitz, *Algebraische Theorie der Körper*, (1930), 17.

$$\alpha'^n + b_1\alpha'^{n-1} + \ldots + r' = 0\,, \tag{1}$$

$$r' = x^n + a_1x^{n-1} + \ldots + rx^i + a_{n-i+1}x^{i-1} + \ldots + a_n\,.$$

Ist $r' \equiv 0\ (\mathfrak{p})$, so folgt daraus

$$x^{n-i} + a_1x^{n-1-i} + \ldots, + r \equiv 0\ (\mathfrak{p})\,. \tag{2}$$

Da $\mathfrak{p}$ aber ein Primideal in $\mathfrak{J}$ ist, so hat (2) in Bezug auf das Primideal $\mathfrak{p}$ nicht mehr als $n-i$ inkongruente Wurzeln in $\mathfrak{J}$. Da $\mathfrak{J} \mid \mathfrak{p}$ aber ein Körper von der Charakteristik 0 ist, so können wir ein durch $\mathfrak{p}$ unteilbares Element $\bar{r}$ in $\mathfrak{J}$ finden, so dass $\bar{r}^{n-i} + a_1\bar{r}^{n-1-i} + \ldots + r \not\equiv 0(\mathfrak{p})$ ist. Damit ist $\varepsilon = \alpha - \bar{r}$ nach (1) eine Einheit. Ist $\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha + a_n = 0$, und sind alle a_i durch $\mathfrak{p}$ teilbar, so wird $\varepsilon' = \alpha - \bar{r}'$ für jedes durch $\mathfrak{p}$ unteilbare Element $\bar{r}'$ aus $\mathfrak{J}$ eine Einheit. Andererseits ist ein durch $\mathfrak{p}$ unteilbares Element aus $\mathfrak{J}$ aber nach der Fussnote in Seite 65 auch eine Einheit. Damit ist unsere Behauptung richtig.