Beweis: Es genügt, den Satz für $n = 2$ zu beweisen, da er dann durch Induktion allgemein folgt. Nach dem (aus den Elementen vorausgesetzten) binomischen Satz ist nun

$$(a_1 + a_2)^p = a_1^p + \sum_{\nu=1}^{p-1} \binom{p}{\nu} a_1^\nu a_2^{p-\nu} + a_2^p ,$$

wo $\binom{p}{\nu}$ die Kombinationsanzahl von p Elementen zur ν-ten Klasse bezeichnet, für die die Formel

$$\binom{p}{\nu} = \frac{p!}{\nu!(p-\nu)!} = \frac{p \cdot (p-1) \cdots (p-(\nu-1))}{1 \cdot 2 \cdots \nu}$$

gilt (vgl. 1, Bew. zu Satz 66 [123]). Da für $1 \leqq \nu \leqq p-1$ das Produkt $1 \cdot 2 \cdots \nu$ zu p prim ist (Satz 23 [22]) und wegen der Ganzzahligkeit der Anzahl $\binom{p}{\nu}$ in dem Produkt $p \cdot [(p-1) \cdots (p-(\nu-1))]$ aufgeht, muß es nach Satz 16 [20] in dem zweiten Faktor $[\ldots]$ dieses Produktes aufgehen, so daß $\binom{p}{\nu} \equiv 0 \bmod p$ ist. Aus Satz 43 folgt daher

$$(a_1 + a_2)^p = a_1^p + a_2^p .$$

Es sei übrigens bemerkt, daß eine entsprechende Regel auch für die Subtraktion gilt; denn aus $(a_1 + a_2)^p - a_1^p = a_2^p$ folgt ja wegen der Unbeschränktheit der Subtraktion allgemein $b_1^p - b_2^p = (b_1 - b_2)^p$.

II. Die Wurzeln algebraischer Gleichungen.

Wir leiten in diesem Abschnitt eine Reihe von Sätzen über Wurzeln α von Polynomen $f(x)$ aus K in Erweiterungskörpern Λ von K her, ohne dabei auf die erst in III zu behandelnde Existenzfrage der Λ und α bei gegebenem K und $f(x)$ einzugehen. Diese Sätze sind also lediglich als Folgerungen aus der Voraussetzung anzusehen, daß ein Polynom aus K in einem Erweiterungskörper Λ von K eine oder mehrere Wurzeln hat.

Zur Vereinfachung der Ausdrucksweise treffen wir folgende

Bezeichnungsfestsetzungen für Abschnitt II—IV.

Große griechische Buchstaben, außer den bereits vergebenen M (Menge), B (Bereich), I (Integritätsbereich), Γ (Integritätsbereich der ganzen Zahlen), bedeuten stets Körper, ohne daß dies immer ausdrücklich gesagt wird, und zwar K den Grundkörper, Λ irgendeinen Erweiterungskörper (kurz Erweiterung) von K, weitere Buchstaben Erweiterungen von K mit speziellen, wie bei P (Körper der rationalen Zahlen) durch die Bezeichnung schon angedeuteten Eigenschaften, die wir aber der Deutlichkeit halber doch immer ausführlich nennen werden. Für das Enthaltensein und Enthalten bei Körpern (später auch bei Gruppen) verwenden wir sinngemäß die Zeichen $\leqq, \geqq, <, >$. Ist $K \leqq \overline{K} \leqq \Lambda$, so nennen wir $\overline{K}$ einen Körper zwischen K und Λ.

Elemente aus dem Grundkörper K bezeichnen wir mit $a, b, c, \ldots$, solche aus Erweiterungen Λ von K mit $\alpha, \beta, \gamma, \ldots$ (vgl. **1**, erste Anm. zu § 1 [9]), ebenso Elemente aus $K[x]$ mit $f(x), g(x), h(x), \ldots$, solche aus $\Lambda[x]$ mit $\varphi(x), \psi(x), \chi(x), \ldots$[1]). Wir dürfen dann erläuternde Zusätze über die Körper, denen vorkommende Elemente angehören sollen, oft fortlassen.

Ebenso lassen wir auch die Zusätze „in K" bei „irreduzibel" und „Primfaktorzerlegung", sowie entsprechende Zusätze bei einigen im weiteren Verlaufe einzuführenden Begriffen, die sich auf einen bestimmten Grundkörper beziehen, gelegentlich fort, wenn nur ein in der gerade vorliegenden Betrachtung fester Grundkörper K in Betracht kommt. Definitionen, auf die diese Festsetzung Anwendung finden soll, werden durch * gekennzeichnet.

§ 5. Wurzeln und Linearfaktoren.

1.) Der in § 1 für $K[x]$ bewiesene Fundamentalsatz ermöglicht zunächst die Herstellung eines Zusammenhangs zwischen den Wurzeln eines Polynoms aus K in einer Erweiterung Λ von K und denen seiner Primfaktoren in K. Nach **1**, Satz 4 [12] und dem Einsetzungsprinzip gilt nämlich:

Satz 45. Ist

$$f(x) \equiv p_1(x) \cdots p_r(x)^{2})$$

ein in seine Primfaktoren zerlegtes Polynom aus

[1]) Vorkommende gebrochene rationale Funktionen, die wir in **1** so bezeichneten, werden als Quotienten ganzer rationaler Funktionen dargestellt.

[2]) Nach der Definition von Polynom i. d. Einl., sowie nach Def. 8 [14] und Satz 11 [14] ist dabei der in Satz 12 [14] auftretende Einheitsfaktor $a = e$.

K, so ist jede Wurzel von $f(x)$ in Λ auch Wurzel von mindestens einem der $p_i(x)$ und umgekehrt jede Wurzel eines der $p_i(x)$ in Λ auch Wurzel von $f(x)$.

Man beherrscht somit die Wurzeln von $f(x)$, wenn man die der $p_i(x)$ beherrscht, und könnte sich demnach auf die Untersuchung der Wurzeln irreduzibler Polynome beschränken. Da sich diese Beschränkung aber für die in III, IV auseinanderzusetzende Theorie als überflüssig erweist, wollen wir sie nicht einführen. Das erscheint auch in Hinsicht auf das Nichtvorhandensein eines rationalen Rechenverfahrens zur Herstellung der Primfaktorzerlegung erwünscht.

2.) Wir beweisen ferner einige Sätze über den Zusammenhang der Wurzeln eines Polynoms aus K mit dessen Primfaktoren 1-ten Grades (sog. **Linearfaktoren**) in einer Erweiterung Λ von K.

Satz 46. Ist α Wurzel von $f(x)$ in Λ, so ist $f(x)$ durch den Linearfaktor $x-\alpha$ teilbar, d. h. es besteht in Λ eine Zerlegung

$$f(x) \equiv (x-\alpha)\,\varphi(x).$$

Umgekehrt folgt aus einer solchen Zerlegung, daß α Wurzel von $f(x)$ ist.

Beweis: a.) Nach Satz 13 [16] kann

$$f(x) \equiv (x-\alpha)\,\varphi(x) + \psi(x) \quad \text{mit} \quad |\psi(x)| < |x-\alpha|$$

gesetzt werden. Da $|x-\alpha| = k^1$ ist, muß $|\psi(x)| = k^0 = 1$ sein, so daß $\psi(x) \equiv \beta$ ein Element aus Λ ist. Für $x = \alpha$ folgt dann wegen $f(\alpha) = 0$ auch $\beta = 0$, d. h. die behauptete Zerlegung.

b.) Die Umkehrung ist klar.

Satz 47. Sind $\alpha_1, \ldots, \alpha_\nu$ verschiedene Wurzeln von $f(x)$ in Λ, so besteht in Λ eine Zerlegung

$$f(x) \equiv (x-\alpha_1)\cdots(x-\alpha_\nu)\,\varphi(x).$$

Umgekehrt folgt aus einer solchen Zerlegung, daß $\alpha_1, \ldots, \alpha_\nu$ Wurzeln von $f(x)$ sind.

Beweis: a.) Die Primfunktionen $x-\alpha_1, \ldots, x-\alpha_\nu$ sind nach Voraussetzung verschieden, und jede kommt nach

Satz 46 in der Primfaktorzerlegung von $f(x)$ im Körper Λ vor. Wegen der Eindeutigkeit dieser Zerlegung muß also auch ihr Produkt in $f(x)$ enthalten sein, d. h. eine Zerlegung der behaupteten Art bestehen.

b.) Die Umkehrung ist klar.

Aus Satz 47 ergibt sich durch Vergleichung der beiderseitigen Grade unmittelbar die wichtige Tatsache:

Satz 48. Ein Polynom n-ten Grades aus K hat in keiner Erweiterung Λ von K mehr als n verschiedene Wurzeln.

Aus Satz 48 läßt sich der folgende, später anzuwendende Satz folgern:

Satz 49. Besteht K aus unendlich vielen Elementen und sind $g_1(x_1, \ldots, x_n), \ldots, g_r(x_1, \ldots, x_n)$ voneinander verschiedene Elemente aus $K[x_1, \ldots, x_n]$, so gibt es in jeder unendlichen Teilmenge M von K Elementsysteme $a_1, \ldots, a_n$ derart, daß die Elemente $g_1(a_1, \ldots, a_n), \ldots, g_r(a_1, \ldots, a_n)$ aus K ebenfalls voneinander verschieden sind.

Beweis: Durch Betrachtung des Differenzenprodukts $g = \prod_{\substack{i,k=1 \\ i<k}}^{r} (g_i - g_k)$ reduziert sich die Behauptung ohne weiteres auf jede der beiden folgenden, gleichbedeutenden:

(a.) Ist $g(x_1, \ldots, x_n) \not\equiv 0$, so gibt es $a_1, \ldots, a_n$ aus M, so daß $g(a_1, \ldots, a_n) \neq 0$ ist.

(b.) Ist $g(a_1, \ldots, a_n) = 0$ für alle $a_1, \ldots, a_n$ aus M, so ist $g(x_1, \ldots, x_n) \equiv 0$ [1]).

Diese beweisen wir durch vollständige Induktion: Für $n = 1$ ist (a.) eine Folge aus Satz 48; ist nämlich $g(x) \not\equiv 0$, so ist entweder $g(x) \equiv b \neq 0$ (Einheit) und also $g(a) = b \neq 0$ für alle a aus M, oder $g(x)$ ist bis auf einen von Null verschiedenen Faktor aus K ein Polynom und dann $g(a) = 0$ für nur endlich viele a aus K, so daß nach den Voraussetzungen über K und M Elemente a in M existieren, für die $g(a) \neq 0$ ist. Sei nun (a.) und somit (b.) für $n = \nu - 1$ schon bewiesen. Dann betrachten wir die Polynome

[1]) Hierdurch wird die in **1**, Bew. zu Satz 12, d) [41] ausgesprochene Behauptung [vgl. dazu **1**, Bew. zu Satz 13, d) [44]] bestätigt. Man hat dazu unter K den Quotientenkörper des dortigen Integritätsbereichs I und unter M das dortige I zu verstehen.

$$\bar{g}(x_\nu) \equiv g(x_1, \ldots, x_\nu) \text{ über } K[x_1, \ldots, x_{\nu-1}],$$
$$\bar{g}^*(x_\nu) \equiv g(a_1, \ldots, a_{\nu-1}, x_\nu) \text{ über } K,$$

von denen die letzteren durch Einsetzung von Systemen $a_1, \ldots, a_{\nu-1}$ aus M für $x_1, \ldots, x_{\nu-1}$ aus dem ersteren entstehen. Ist nun $g(a_1, \ldots, a_\nu) = 0$ für alle $a_1, \ldots, a_\nu$ aus M, so ist nach (b.) $(n = 1)$ zunächst jedes $\bar{g}^*(x_\nu) \equiv 0$. Folglich sind nach (b.) $(n = \nu - 1)$ die Koeffizienten von $\bar{g}(x_\nu)$, d. h. $\bar{g}(x_\nu)$ selbst $\equiv 0$, was $g(x_1, \ldots, x_\nu) \equiv 0$ bedeutet. Also ist (b.) dann auch für $n = \nu$, und daher allgemein richtig.

Präziser als Satz 47, 48, insofern nicht mehr die Verschiedenheit der Wurzeln vorausgesetzt wird, ist der folgende Satz:

Satz 50. Zerfällt $f(x)$ in Λ in Linearfaktoren:

$$f(x) \equiv (x - \alpha_1) \cdots (x - \alpha_n),$$

so sind $\alpha_1, \ldots, \alpha_n$ Wurzeln von $f(x)$. Weitere Wurzeln von $f(x)$ existieren dann weder in Λ noch in irgendeiner Erweiterung Λ von Λ.

Beweis: a.) Der erste Teil des Satzes ist klar (Satz 47 [40]).

b.) Ist α Wurzel von $f(x)$ (in Λ oder einem $\overline{\Lambda}$), so folgt aus $f(\alpha) = 0$, daß $(\alpha - \alpha_1) \cdots (\alpha - \alpha_n) = 0$ ist, so daß α einer der Wurzeln α_i gleich sein muß (1, Satz 4 [12]).

Wir verabreden für die Folge, daß bei der Voraussetzung von Satz 50 unter den Wurzeln von $f(x)$ in Λ stets die den Linearfaktoren von $f(x)$ entsprechende volle Reihe $\alpha_1, \ldots, \alpha_n$ verstanden wird, ungeachtet ob darunter gleiche vorkommen oder nicht.

Durch die Sätze 46, 47, 50 ist der Weg für die in III auszuführende Konstruktion der Wurzeln eines Polynoms $f(x)$ aus K vorgezeichnet. Wir werden K schrittweise so zu erweitern haben, daß von $f(x)$ bei jedem Schritt mindestens ein Linearfaktor abgespalten wird. Ist auf diese Weise eine Erweiterung Λ gefunden, in der $f(x)$ vollständig in Linearfaktoren zerfällt, so dürfen wir mit dem Erweiterungsprozeß haltmachen, da eine Fortsetzung dann nach Satz 50 keine neuen Wurzeln mehr liefern kann.

3.) Wir beweisen schließlich einige Tatsachen über die Wurzeln irreduzibler Polynome.

Aus Satz 46 [40] und dem Begriff der Irreduzibilität folgt zunächst unmittelbar:

Satz 51. Ein irreduzibles Polynom aus K hat in K dann und nur dann eine Wurzel, wenn es vom Grade 1 ist.

Hierdurch wird der in der Einleitung hervorgehobene Umstand 2.) in Evidenz gesetzt, daß man i. a. den Grundkörper erweitern muß, um zu Wurzeln eines Polynoms zu gelangen. Man muß allerdings die hier nicht vollständig zu erörternde Tatsache hinzunehmen, daß der Grundkörper i. a. irreduzible Polynome von höherem als dem 1-ten Grade enthält. (Spezielle Sätze in dieser Richtung siehe in § 23.)

Satz 52. Zwei relativ prime Polynome, insbesondere also zwei verschiedene irreduzible Polynome aus K haben in keiner Erweiterung von K eine gemeinsame Wurzel.

Beweis: Ist α eine gemeinsame Wurzel von $f_1(x)$ und $f_2(x)$ in Λ, so ist $x-\alpha$ nach Satz 46 [40] ein gemeinsamer Teiler von $f_1(x)$ und $f_2(x)$ in Λ. Nach Satz 24 [23] ist dann also $(f_1(x), f_2(x)) \neq e$.

Aus Satz 52 ergibt sich der folgende sog. **Fundamentalsatz über irreduzible Polynome:**

Satz 53. Hat das in K irreduzible $f(x)$ mit irgendeinem $h(x)$ aus K in einer Erweiterung von K eine gemeinsame Wurzel, so ist $f(x) \mid h(x)$.

Beweis: Nach Satz 17 [20] wäre sonst $f(x)$ prim zu $h(x)$, was nach Satz 52 der Voraussetzung widerspricht.

In diesem Satz braucht $h(x)$ nicht ein Polynom, also von 0 und Einheiten verschieden und normiert zu sein. Insbesondere wird der Satz für $h(x) \equiv 0$ trivial, für $h(x) \equiv a$ inhaltlos.

Auf Satz 53 wird sich unsere in III auszuführende Konstruktion der Wurzeln von $f(x)$ vornehmlich stützen.

§ 6. Mehrfache Wurzeln, Ableitung.

Definition 15. Eine Wurzel α von $f(x)$ in Λ heißt **ν-fach,** wenn in Λ (und somit in jeder Erweiterung

von Λ) eine Zerlegung

$$f(x) \equiv (x-\alpha)^{\nu} \varphi(x) \quad \text{mit} \quad \varphi(\alpha) \neq 0$$

besteht; **mehrfach,** wenn $\nu > 1$ ist.

Die Bezeichnung ν-fach rechtfertigt sich durch die Tatsache:

Satz 54. Ist α eine ν-fache Wurzel von $f(x)$ in Λ, so sind genau ν Wurzeln von $f(x)$ in Λ (und in jeder Erweiterung von Λ) gleich α.

Beweis: Nach Def. 15 enthält dann $f(x)$ den Primfaktor $x-\alpha$ mindestens ν-mal, wegen $\varphi(\alpha) \neq 0$ aber nach Satz 46 [40] nicht öfter.

Die Vielfachheit einer Wurzel von $f(x)$ steht in Zusammenhang mit der aus der Analysis bekannten Ableitung $f'(x)$ von $f(x)$. Natürlich können wir die Ableitung hier, für unsere abstrakten Grundkörper nicht auf die in der Analysis übliche Weise durch einen Grenzprozeß definieren. Wir geben daher die folgende, formale Definition:

Definition 16. Unter der **Ableitung** von

$$f(x) \equiv a_0 + a_1 x + \cdots + a_n x^n \equiv \sum_{k=0}^{\infty} a_k x^k \text{ [1]}$$

verstehen wir

$$f'(x) \equiv a_1 + 2a_2 x + \cdots + n a_n x^{n-1} \equiv \sum_{k=1}^{\infty} k a_k x^{k-1}$$

$$\equiv \sum_{k=0}^{\infty} (k+1) a_{k+1} x^k.$$

Für diesen formal mit der entsprechenden Differentiationsregel der Analysis übereinstimmenden Prozeß der Ableitungsbildung gelten wie dort die Formeln

(1.) $$(f(x) \pm g(x))' \equiv f'(x) \pm g'(x),$$

(2.) $$(f(x)\, g(x))' \equiv f'(x)\, g(x) + f(x)\, g'(x),$$

insbesondere also

$$(af(x))' \equiv a f'(x),$$

$$(f(x)^n)' \equiv n f(x)^{n-1} f'(x).$$

Beweis: Ist

[1]) Vgl. I, Anm. 3 zu Satz 11 [32].

$$f(x) \equiv \sum_{k=0}^{\infty} a_k x^k, \qquad g(x) \equiv \sum_{k=0}^{\infty} b_k x^k,$$

also

$$f'(x) \equiv \sum_{k=1}^{\infty} k a_k x^{k-1} \equiv \sum_{k=0}^{\infty} (k+1)\, a_{k+1} x^k,$$

$$g'(x) \equiv \sum_{k=1}^{\infty} k b_k x^{k-1} \equiv \sum_{k=0}^{\infty} (k+1)\, b_{k+1} x^k,$$

so folgt nach **1**, § 4, (2.), (3.) [33] (vgl. auch **1**, Schluß von § 1 [13])

$$(f(x)+g(x))' \equiv \Big(\sum_{k=0}^{\infty} (a_k+b_k) x^k\Big)' \equiv \sum_{k=1}^{\infty} k(a_k+b_k) x^{k-1}$$

$$\equiv \sum_{k=1}^{\infty} k a_k x^{k-1} + \sum_{k=1}^{\infty} k b_k x^{k-1} \equiv f'(x)+g'(x),$$

$$(f(x)\, g(x))' \equiv \Big(\sum_{k=0}^{\infty} \Big(\sum_{\nu+\mu=k} a_\nu b_\mu\Big) x^k\Big)' \equiv \sum_{k=1}^{\infty} \Big(k \sum_{\nu+\mu=k} a_\nu b_\mu\Big) x^{k-1}$$

$$\equiv \sum_{k=1}^{\infty} \Big(\sum_{\nu+\mu=k} (\nu+\mu)\, a_\nu b_\mu\Big) x^{k-1}$$

$$\equiv \sum_{k=1}^{\infty} \Big(\sum_{\nu+\mu=k} \nu a_\nu b_\mu\Big) x^{k-1} + \sum_{k=1}^{\infty} \Big(\sum_{\nu+\mu=k} \mu a_\nu b_\mu\Big) x^{k-1}$$

$$\equiv \sum_{k=0}^{\infty} \Big(\sum_{\nu+\mu=k} (\nu+1)\, a_{\nu+1} b_\mu\Big) x^k + \sum_{k=0}^{\infty} \Big(\sum_{\nu+\mu=k} (\mu+1)\, a_\nu b_{\mu+1}\Big) x^k$$

$$\equiv f'(x)\, g(x) + f(x)\, g'(x).$$

Ferner gilt, sozusagen als Ersatz für die fehlende Grenzrelation:

Satz 55. Wird für ein α

$$\varphi(x) \equiv \frac{f(x)-f(\alpha)}{x-\alpha}$$

gesetzt, so ist

$$\varphi(\alpha) = f'(\alpha).$$

Beweis: Da α Wurzel von $f(x)-f(\alpha)$ ist, ist $\varphi(x)$ nach Satz 46 [40] wirklich eine ganze rationale Funktion. Aus

$$f(x) \equiv f(\alpha) + (x-\alpha)\, \varphi(x)$$

folgt daher nach (1.), (2.)

$$f'(x) \equiv \varphi(x) + (x-\alpha)\, \varphi'(x),$$

also

$$f'(\alpha) = \varphi(\alpha).$$

Aus Satz 55 ergibt sich nun der folgende Zusammenhang zwischen der Mehrfachheit einer Wurzel α von $f(x)$ und dem Ableitungswert $f'(\alpha)$:

Satz 56. Eine Wurzel α von $f(x)$ ist dann und nur dann mehrfach, wenn $f'(\alpha) = 0$ ist.

Beweis: Ist α Wurzel von $f(x)$, so hat in der nach Satz 46 [40] bestehenden Zerlegung

$$f(x) \equiv (x - \alpha)\, \varphi(x)$$

$\varphi(x)$ dieselbe Bedeutung wie in Satz 55. Nun ist nach Def. 15 [43] die Mehrfachheit von α mit $\varphi(\alpha) = 0$, also nach Satz 55 mit $f'(\alpha) = 0$ gleichbedeutend.

Der hierin liegende Zusammenhang führt zu einer wichtigen Folgerung über die Vielfachheit der Wurzeln eines irreduziblen Polynoms. Diese Folgerung beruht auf dem Analogon zu dem Satz der Analysis, daß aus $f'(x) \equiv 0$ folgt $f(x) \equiv a_0$. Wegen des Auftretens der ganzen Vielfachen ka_k der a_k als Koeffizienten von $f'(x)$ findet aber hier eine Abweichung gegenüber der Analysis statt:

Satz 57. Hat K die Charakteristik 0, so haben alle und nur die Einheiten $f(x) \equiv a_0$ aus $\mathsf{K}[x]$ die Ableitung $f'(x) \equiv 0$. Hat K die Charakteristik p, so haben alle und nur die Elemente von der Form

$$(3.) \qquad f(x) \equiv \sum_{l=0}^{\infty} a_{lp}\, x^{lp}, \text{ also } f(x) \equiv f_0(x^p)$$

aus $\mathsf{K}[x]$ die Ableitung $f'(x) \equiv 0$.

Beweis: a.) Daß für die genannten $f(x)$ durchweg $f'(x) \equiv 0$ ist, ist nach Satz 43 [37] und Def. 16 [44] klar.

b.) Ist $f(x) \equiv \sum_{k=0}^{\infty} a_k x^k$ und ist $f'(x) \equiv \sum_{k=1}^{\infty} k a_k x^{k-1} \equiv 0$, also $ka_k = 0$ $(k = 1, 2, \ldots)$, so folgt nach Satz 43 im Falle der Charakteristik 0

$$a_k = 0 \qquad (k = 1, 2, \ldots),$$

d. h. $f(x) \equiv a_0$, im Falle der Charakteristik p dagegen nur $a_k = 0$ für $k \not\equiv 0 \bmod p$,
so daß $f(x)$ von der Form (3.) ist.

Die in Satz 57 liegende Abweichung für den Fall der Charakteristik p bedingt nun, daß die angekündigte Folgerung über die Vielfachheit der Wurzeln eines irreduziblen Polynoms im Fall der Charakteristik p auf solche irreduziblen Polynome zu beschränken ist, die nicht von der Form (3.) sind. Steinitz[1]) nennt solche irreduziblen Polynome von erster Art, die von der Form (3.) von zweiter Art.

Dem Vorgang v. d. Waerdens folgend, wollen wir die in der nachstehenden Definition gegebene Bezeichnung gebrauchen:

Definition 17. Ein **irreduzibles Polynom** $f(x)$ aus K heißt **separabel,** wenn seine Ableitung $f'(x) \not\equiv 0$ ist, also, falls K die Charakteristik 0 hat, stets; falls K die Charakteristik p hat, dann und nur dann, wenn es nicht von der Form (3.) in Satz 57 ist.

Andernfalls heißt $f(x)$ **inseparabel.**

Die Bezeichnung separabel spielt auf die folgende Tatsache, die bereits angekündigte Folgerung aus Satz 56, an:

Satz 58. Ist ein irreduzibles Polynom $f(x)$ separabel, so hat $f(x)$ nur einfache Wurzeln.

Beweis: Wäre α eine mehrfache Wurzel von $f(x)$, so wäre $f'(\alpha) = 0$ (Satz 56) und daher $f(x) \mid f'(x)$ (Satz 53 [43]). Wegen der vorausgesetzten Separabilität von $f(x)$ ist nun $f'(x) \not\equiv 0$ (Def. 17). $f'(x)$ kommt also ein Grad zu, und dieser ist kleiner als der von $f(x)$ (Def. 16 [44]). Das steht aber im Widerspruch zu $f(x) \mid f'(x)$ (Satz 6 [13]). Also ist die Annahme, $f(x)$ habe eine mehrfache Wurzel, unzutreffend.

[1]) Wir meinen bei Nennung des Namens Steinitz hier und im folgenden stets dessen in **1**, Lit. Verz. I zitierte Arbeit, deren Abschnitte I und II bis auf das die Erweiterungen zweiter Art Betreffende in unseren Abschnitten **1**, I und **2**, I—IV verarbeitet sind, ja geradezu deren Inhalt ausmachen. In diese grundlegende Originalarbeit zur Körpertheorie sollte jeder Algebraiker einmal hineingesehen haben.

Satz 58 läßt übrigens folgende Umkehrung zu:

Satz 59. Hat ein irreduzibles Polynom $f(x)$ eine nur einfache Wurzel α, so ist $f(x)$ separabel.

Beweis: Es ist dann $f'(\alpha) \neq 0$ (Satz 56), also gewiß $f'(x) \not\equiv 0$, und daher $f(x)$ separabel (Def. 17).

Wir definieren ferner noch im Anschluß an Def. 17:

***Zusatz zu Definition 17** [1]). Ein **beliebiges Polynom** aus K heißt **separabel** in K, wenn seine Primfaktoren in K separabel sind, sonst **inseparabel** in K.

Im Falle der Charakteristik 0 ist also jedes Polynom separabel. Für den Fall der Charakteristik p sei ausdrücklich bemerkt, daß die Entscheidung über die Separabilität beliebiger Polynome nicht etwa, wie gemäß Def. 17 für irreduzible Polynome, einfach durch Bilden der Ableitung getroffen werden kann. Es kann sehr wohl $f'(x) \equiv 0$ auch für separables $f(x)$ sein (z. B. wenn $f(x) \equiv f_0(x)^p$ mit separablem irreduziblem $f_0(x)$ ist), und $f'(x) \not\equiv 0$ für inseparables $f(x)$ (z. B. wenn $f(x) \equiv x f_0(x)$ mit inseparablem irreduziblem $f_0(x)$ ist). Auch der in Satz 58, 59 gegebene Zusammenhang mit der Wurzelvielfachheit, der die Bezeichnung separabel rechtfertigte, überträgt sich nicht auf beliebige Polynome. Dennoch ist die im Zusatz zu Def. 17 gegebene Ausdehnung dieser Bezeichnung auf beliebige Polynome für die späteren Zwecke nützlich.

Über ein Verfahren zur Entscheidung über die Separabilität beliebiger Polynome, das nicht die Zerlegung in Primfaktoren erfordert (was nach dem im Anschluß an Satz 24 [23] Gesagten erwünscht sein muß), sei des knappen Raumes halber auf Steinitz verwiesen. Hier sei nur die folgende für unsere Zwecke ausreichende Tatsache vermerkt, die sich gemäß Def. 17, Zusatz unmittelbar aus Satz 59 ergibt:

Zusatz zu Satz 59. Zerfällt ein beliebiges Polynom $f(x)$ aus K in einer Erweiterung von K in verschiedene Linearfaktoren, d. h. sind die Wurzeln $\alpha_1, \ldots, \alpha_n$ von

$$f(x) \equiv (x - \alpha_1) \cdots (x - \alpha_n)$$

voneinander verschieden, so ist $f(x)$ separabel (in K und jeder Erweiterung von K).

[1]) Über die Bedeutung von * vgl. die Einl. zu II [39].

Von Bedeutung sind diejenigen Körper, in denen jedes Polynom separabel ist. Sie heißen vollkommene Körper. Wir wollen unter Benutzung teilweise erst später zu gewinnender Resultate ganz kurz einige Angaben über vollkommene Körper machen.

Zunächst ist jeder Körper der Charakteristik 0 vollkommen, wie wir den obigen Betrachtungen unmittelbar entnehmen können. — Soll ferner ein Körper K der Primzahlcharakteristik p vollkommen sein, so muß insbesondere jedes Polynom $x^p - a$ aus K separabel sein. Dann ist die Gleichung $x^p \doteq a$ in K lösbar. Denn aus ihrer Unlösbarkeit in K folgte nach dem späteren Satz 123, b.) [137] die Irreduzibilität des Polynoms $x^p - a$ in K und daher nach Def. 17 seine Inseparabilität. Die Lösung von $x^p \doteq a$ in K ist überdies eindeutig. Aus $a_1^p = a, a_2^p = a$ folgt ja $0 = a_1^p - a_2^p = (a_1 - a_2)^p$ (Satz 44 [37]), also $a_1 - a_2 = 0, a_1 = a_2$. Wir bezeichnen diese eindeutige Lösung von $x^p \doteq a$ mit $\sqrt[p]{a}$.

Sei umgekehrt in dem Körper K der Primzahlcharakteristik p die Gleichung $x^p \doteq a$ für jedes a aus K lösbar. Wäre dann das irreduzible Polynom $f(x)$ aus K inseparabel, so wäre $f(x)$ nach Def. 17 von der Form

$$f(x) = \sum_{\nu=0}^{n} a_\nu x^{\nu p} = \sum_{\nu=0}^{n} \left(\sqrt[p]{a_\nu}\right)^p x^{\nu p},$$

und Satz 44 [37] lieferte

$$f(x) = \left(\sum_{\nu=0}^{n} \sqrt[p]{a_\nu}\, x\right)^p,$$

im Widerspruch zur Irreduzibilität von $f(x)$. — Wir haben demnach gefunden:

Ein Körper K der Primzahlcharakteristik p ist dann und nur dann vollkommen, wenn mit a stets auch $\sqrt[p]{a}$ in K enthalten ist.

Hiernach und nach Satz 29 [29] sind die Primkörper P_p vollkommene Körper. — Daß nicht jeder Körper vollkommen ist, d. h. daß es sogenannte unvollkommene Körper gibt, zeigt das Beispiel $P_p(x)$; denn dieser Körper hat die Charakteristik p, und das Element x besitzt keine p-te Wurzel in ihm. Wäre nämlich $\left(\frac{f(x)}{g(x)}\right)^p \equiv x$, d. h. $(f(x))^p \equiv x(g(x))^p$ (wobei natürlich $f(x)$, $g(x) \not\equiv 0$ sein müßten), und wären n, m die Grade von $f(x)$, $g(x)$, so folgte nach § 1, B., (3.) [12] $pm = 1 + pm$, d. h. $0 \equiv 1 \bmod p$, was nicht der Fall ist.