Sitzungsberichte

der

mathematisch-naturwissenschaftlichen Abteilung

der

Bayerischen Akademie der Wissenschaften

zu München

1928. Heft III

November-Dezembersitzung

München 1928

Verlag der Bayerischen Akademie der Wissenschaften

in Kommission des Verlags R. Oldenbourg München

Über einen Satz von E. Steinitz.

Von **Otto Haupt**, Erlangen.

Vorgelegt von Georg Faber in der Sitzung am 15. Dezember.

1. Vorbemerkung: Es sei K ein Körper der Charakteristik $p \geq 2$[1]). Die Frage, ob bzw. wann jede Erweiterung 2. Art von K Radikale p-ten Grades über dem Grundkörper, nämlich über K enthält, wurde wohl zuerst von R. Hölzer behandelt und von E. Steinitz beantwortet. Letzterer teilte mir hierüber folgendes mit[2]): „Übrigens habe ich, durch die Hölzer'sche Vermutung angeregt, damals einige Zeit die Untersuchungen über unvollkommene Körper wieder aufgenommen und erlaube mir, Ihnen die Ergebnisse, die sich auf die Hölzer'sche Frage beziehen, mitzuteilen. Es gibt unvollkommene Körper, für die die Hölzer'sche Vermutung zutrifft, bei denen also jede Erweiterung 2. Art p-te Radikale über K enthält. Es ist dies dann und nur dann der Fall, wenn für jedes irreduzible Polynom $x^n + a_1 x^{n-1} + \ldots + a_n$ aus K gilt, daß, falls nicht $\sqrt[p]{a_1}, \ldots, \sqrt[p]{a_n}$ sämtlich zu K gehören, $K(\sqrt[p]{a_1}, \ldots, \sqrt[p]{a_n})$ über K vom Grade p ist. Es fragt sich aber, wie man diese Körper näher charakterisieren kann. Da zeigt sich, daß es zwei Arten solcher Körper (bei denen die Hölzer'sche Vermutung zutrifft) gibt. Erstens diejenigen, für welche K über K_1 von Grade p ist[3]) (Körper dieser Art erhält man z. B., indem man einem vollkommenen Körper von der Charakteristik p ein transzendentes Element adjungiert). Zweitens diejenigen, bei denen jede algebraische Er-

---

[1]) Für die im folgenden gebrauchten Bezeichnungen vgl. Haupt, Einführung in die Algebra (Leipzig, 1929), abgekürzt zitiert mit A.

[2]) Brief vom 24. IX. 27. In der nachstehenden wörtlichen Wiedergabe sind nur einige Bezeichnungen geändert.

[3]) K_1 bezeichnet den Körper der p-ten Potenzen aller Elemente von K (vgl. A., Nr. 6, 8; Satz 4). Falls $K = K_1$ ist, heißt K „vollkommen", sonst „unvollkommen".

weiterung ein Wurzelkörper[1]) ist. (Um einen solchen Körper zu erhalten, geht man von einem beliebigen unvollkommenen Körper K aus. Ist N die algebraisch abgeschlossene, algebraische Erweiterung von K, Λ der Körper zwischen K und N, der die Elemente von N umfaßt, die in Bezug auf K von 1. Art sind, so hat jeder Körper T zwischen Λ und N die geforderte Eigenschaft.) Schwierig ist der Beweis, daß mit diesen beiden Arten alle „Hölzerschen Körper" erschöpft sind." Soweit der Steinitz'sche Brief. Den am Schlusse von ihm erwähnten Beweis teilte mir Steinitz nicht mit; übrigens ist meines Wissens ein Beweis für den Steinitzschen Satz bisher überhaupt nicht veröffentlicht worden. Deshalb dürfte ein (wohl als einfach zu bezeichnender) Beweis, welchen ich inzwischen gefunden habe (vgl. weiter unten 3., Satz 2, Bew.), nicht ohne Interesse sein.

2. Wir erinnern zunächst an folgende bekannte Tatsachen, auf die wir uns später zu berufen haben:

I. Es bezeichne K einen unvollkommenen Körper der Charakteristik $p \geq 2$, ferner K_1 den Körper der p-ten Potenzen aller Elemente von K. Polynome $P(x)$, deren Koeffizienten Elemente aus K (bzw. K_1) sind, heißen Polynome über K (bzw. K_1) oder auch Polynome aus $K[x]$ (bzw. $K_1[x]$). Die im Folgenden betrachteten Polynome sollen übrigens ausnahmslos so normiert sein, daß der Koeffizient der höchsten Potenz von x Eins ist. Ein über K irreduzibles Polynom $P(x)$ heißt von 1. Art, wenn $P(x)$ nur einfache Wurzeln besitzt; sonst von 2. Art.

Ist $P(x) = Q(x^{p^l})$ von 2. Art und vom Exponenten l über K ($l \geq 1$), so ist $Q(y)$ von 1. Art über K (vgl. A., Nr. 13, 3); überdies kann $P(x)$, und damit $Q(y)$, nicht zu $K_1[x]$ gehören, weil andernfalls $P(x)$ die p-te Potenz eines Polynoms aus $K[x]$, also $P(x)$ reduzibel über K wäre. — Ist umgekehrt $R(y)$ vom Grade n und von 1. Art über K und gehört $R(y)$ nicht zu $K_1[x]$, so ist $F(x) = S(x^{p^t})$ von 2. Art über K ($t \geq 1$ beliebige natürliche Zahl). Denn wäre $F(x)$ reduzibel über K und etwa $F_1(x)$ ein irreduzibler (echter) Teiler von $F(x)$ über K, so hätte auch $F_1(x)$ den reduzierten Grad n, es wäre $F(x) = [F_1(x)]^\pi$, wo

[1]) Auch „Radikalkörper", vgl. im Text weiter unten (2., II.).

$\pi = p^s$, $s \geq 1$, und $F(x)$ gehörte zu $K_1[x]$ gegen die Voraussetzung.

Aus dem über Polynome 1. u. 2. Art Gesagten folgt: Das Koeffizientensystem eines jeden, nicht zu $K_1[x]$ gehörigen (normierten) Polynoms 1. Art ist auch Koeffizientensystem von Polynomen 2. Art und umgekehrt.

II. Eine Erweiterung Λ von K heiße „Radikalkörper" über K, wenn jedes Element a aus Λ ein π-tes Radikal, d. h. Wurzel eines irreduziblen Binoms $x^\pi - a$ über K ist, wo $\pi = p^r$ eine zu a passend gewählte Potenz von p bedeutet ($r \geq 1$). Ist der Radikalkörper Λ vom Grade p über K (Zeichen: $[\Lambda : K] = p$), so ist jedes nicht zu K gehörige Element a von Λ ein p-tes Radikal über K; ferner gilt $\Lambda = K(a)$, falls a nicht zu K gehört. Ordnet man jedem Element von Λ seine p-te Potenz zu, so wird K isomorph auf K_1 abgebildet (vgl. A., Nr. 6, 8) und gleichzeitig Λ isomorph auf einen, in K enthaltenen Radikalkörper R vom Grade p über K_1 (falls $[\Lambda : K] = p$). Übrigens ist R primitiv über K_1, sodaß zwei beliebige derartige Radikalkörper R_1 und R_2 entweder identisch sind oder elementenfremd (vgl. A., Nr. 6, 5) über K_1.

Sind $b_1, \ldots, b_n$ Elemente aus K, so sind $\sqrt[p]{b_1}, \ldots, \sqrt[p]{b_n}$ dann und nur dann sämtlich in einem Radikalkörper p-ten Grades über K (aber nicht sämtlich in K) enthalten wenn $[K(\sqrt[p]{b_1}, \ldots, \sqrt[p]{b_n}) : K] = p$ ist, oder, was damit gleichbedeutend, wenn $b_1, \ldots, b_n$ zum nämlichen Radikalkörper R vom Grade p über K_1 (aber nicht sämtlich zu K_1) gehören; falls etwa $[K_1(b_1) : K_1] = p$ ist, gilt $K(b_1) = K(b_1, \ldots, b_n)$.

3. Den Ausgangspunkt für den Beweis des Steinitz'schen Satzes bildet (vgl. auch 1.) der

1. Satz: Es sei $M = K(\beta)$ eine einfache Erweiterung von 2. Art über K; dabei sei β etwa Wurzel von $P(x)$ über K. Damit M ein Radikal $\alpha = \sqrt[p]{a}$ vom Grade p über K enthalte, ist notwendig und hinreichend, daß die Koeffizienten von $P(x)$ sämtlich zum Radikalkörper $R = K_1(a)$ vom Grade p über K_1 gehören[1]).

[1]) Zufolge 2., I. gehören nicht alle Koeffizienten zu K_1, weil $P(x)$ von 2. Art über K ist. (Betr. Erweiterungen 2. Art vgl. etwa A., Nr. 23, 2.)

Beweis: A) Damit α in M enthalten sei, ist notwendig und hinreichend, daß $P(x)$ über $K(\alpha)$ reduzibel wird. Die Bedingung ist notwendig, weil $[\alpha : K] = p$ ist, also $[\beta : K(\alpha)] < [\beta : K]$ sein muß, falls α in M enthalten ist. Die Bedingung ist aber auch hinreichend: Es zerfalle nämlich $P(x)$ über $K(\alpha)$. Dann zerfällt nach dem Kronecker-Kneser'schen Satz (vgl. A., Nr. 17, 6) auch $B(x) = x^p - a$ über $K(\beta)$; aber $B(x)$ zerfällt als Normalpolynom von Primzahlgrad in lauter Linearfaktoren (vgl. A., Nr. 21, 2; oder Nr. 13, 3; Satz 3, Bew.). Mithin ist a in $K(\beta)$ enthalten.

B) Damit $P(x)$ über $K(\alpha)$ reduzibel werde, ist notwendig, daß $P(x) = [P_1(x; \alpha)]^p$, wo $P_1(x; \alpha)$ irreduzibler Teiler von $P(x)$ über $K(\alpha)$ ist; jeder Primteiler $P_1(x; \alpha)$ muß nämlich den reduzierten Grad n besitzen, woraus wegen $[\beta : K(\alpha)] = n\, p^{l-1}$ (vgl. A) die Behauptung folgt. Daß dies auch hinreicht, ist trivial. Nun gilt aber eine Relation $P(x) = [S(x; \alpha)]^p$ dann und nur dann, wenn die Koeffizienten von $P(x)$ sämtlich p-te Potenzen von Elementen aus $K(\alpha)$ sind; gleichbedeutend damit ist zufolge 2., II., daß die Koeffizienten von $P(x)$ zu $R = K_1(a)$ gehören w. z. z. w.

Mit Hilfe des 1. Satzes erhält man jetzt den Beweis des Steinitzschen Satzes. Bezeichnen wir zur Abkürzung als „Hölzer'schen Körper" einen (unvollkommenen) Körper K von der Eigenschaft, daß jede Erweiterung 2. Art über K (mindestens) ein Radikal p-ten Grades über K enthält, so lautet die Behauptung von Steinitz:

2. Satz: K ist ein Hölzer'scher Körper dann und nur dann, wenn entweder K über K_1 den Grad p hat, oder, wenn jede algebraische Erweiterung von K ein Radikalkörper ist.

Beweis: Notwendig und hinreichend ist jedenfalls, daß jede einfache Erweiterung 2. Art über K ein Radikal p-ten Grades über K enthält. Nach dem 1. Satze tritt dies aber dann und nur dann ein, wenn die Koeffizienten eines beliebigen Polynoms 2. Art über K jeweils sämtlich einem Radikalkörper R vom Grade p über K_1 angehören. Gemäß 1., I. ist aber diese Bedingung gleichbedeutend damit, daß überhaupt für jedes über K irreduzible, nicht zu $K_1[x]$ gehörige, Polynom die Koeffizienten jeweils sämtlich zu einem R gehören.

Im Falle $[K : K_1] = p$ ist nun (vgl. 2., II.) nur ein R vorhanden ($R = K$), also K ein Hölzer'scher Körper. Ist hingegen[1]) $[K : K_1] \geq p^2$, so kann — dem soeben Bewiesenen zufolge — K ein Hölzer'scher Körper nur dann sein, wenn ein nicht-lineares, nicht zu $K_1[x]$ gehöriges, Polynom $P(x)$ über K reduzibel ist, sobald nur $P(x)$ Koeffizienten aus mindestens zwei verschiedenen Radikalkörpern vom Grade p über K_1 (etwa aus R_1 und R_2) besitzt ($R_1 \neq R_2$). Zum Beweise des 2. Satzes genügt deshalb der Nachweis, daß jedes nicht durch x teilbare, nicht-lineare Polynom $H(x)$ über K, welches kein Binom p^l-ten Grades ist ($l > 1$), sich in ein, nicht zu $K_1[y]$ gehöriges, Polynom $Q(y)$ mit (nicht zu K_1 gehörigen) Koeffizienten aus R_1 und R_2 überführen läßt ($R_1 \neq R_2$) vermöge einer (ganzen) linearen Transformation $y = a_1 x + a_2$ ($a_1 \neq 0$; a_1, a_2 Elemente aus K). Da nämlich bei derartiger linearer Transformation (der Unbestimmten x) jedes über K irreduzible Polynom wieder in ein über K irreduzibles vom gleichen Grade übergeht, und da die Transformation ein-eindeutig ist, so folgt: K kann, falls $[K : K_1] \geq p^2$ ist, ein Hölzer'scher Körper nur dann sein, wenn jedes nicht lineare, von einem Binom p^l-ten Grades ($l \geq 1$) verschiedene Polynom über K reduzibel ist, wenn also als algebraische Erweiterungen von K nur Radikalkörper in Frage kommen. Ein solcher Körper K ist aber auch wirklich ein Hölzer'scher Körper.

Lineare Transformationen der in Rede stehenden Art gewinnt man etwa durch folgende Überlegungen: Es sei $[K : K_1] \geq p^2$ und es seien R_1, R_2 zwei verschiedene Radikalkörper p-ten Grades über K_1 in K. Schließlich sei

$$P(x) = x^n + a_1 x^{n-1} + \ldots + a_n, \quad a_n \neq 0$$

ein nicht-lineares Polynom über K, dessen Koeffizienten alle zu R_1 oder ev. sogar alle zu K_1 gehören ($n \geq 2$).

Wir unterscheiden zwei Fälle:

1. Fall: $n \not\equiv 0 \pmod{p}$.

a) Wir können $a_1 = 0$ annehmen; ist nämlich $a_1 \neq 0$, so können wir $P(x)$ durch die Substitution $x = y - (n \times \varepsilon)^{-1} \cdot a_1$

[1]) Man beachte, daß $[K : K_1]$ stets eine Potenz von p sein muß, es sei denn, daß K über K_1 gar nicht endliche Erweiterung ist. Dieser letztere Fall soll bei der Aussage $[K : K_1] \geq p^2$ stets mit einbezogen sein.

in ein Polynom $R(y)$ vom Grade n in y über K transformieren, in welchem der Koeffizient von y^{n-1} Null ist. Ferner können wir stets erreichen, daß $P(x)$ nicht zu $K_1[x]$ gehört; denn andernfalls erhalten wir durch die Substitution $x = cz$ (wobei c ein beliebiges, nicht zu K_1 gehöriges, Element aus R_1 bezeichnet) das Polynom $c^{-n} P(cz) = F(z)$ in z über K, in welchem der Koeffizient von z^0 gleich $a_n c^{-n}$ ist und (wegen $n \not\equiv 0 \pmod{p}$) gewiß nicht zu K_1 gehört, wenn $a_n \neq 0$ in K_1 liegt.

b) Zufolge a) können wir zu $P(x) = x^n + a_2 x^{n-2} + \ldots + a_n$ einen kleinsten Index $r \geq 2$ angeben, sodaß a_r nicht zu K_1 gehört, also insbesondere von Null verschieden ist. Gehört a_r, ebenso wie alle übrigen Koeffizienten von $P(x)$, etwa zu R_1, so transformieren wir $P(x)$ vermöge $x = y + f$, wobei f ein nicht in R_1 gelegenes Element aus K, etwa aus R_2 bedeutet. Wir erhalten:

$$P(y+f) = H(y) = y^n + (n \times f) y^{n-1} + \ldots + [a_r + Q(f)] y^{n-r} + \ldots,$$
$$2 < r < n.$$

Dabei ist $Q(f)$ ein Polynom in f über K_1, weil $Q(f)$ nur von den, dem $a_r x^r$ in $P(x)$ vorangehenden Gliedern $x^n, \ldots, a_{r-1} x^{n-r+1}$ herrührt und weil deren Koeffizienten sämtlich zu K_1 gehören. Infolgedessen gehört $a_r + Q(f)$ weder zu K_1 noch zu R_2, während $(n \times f)$ in R_2 liegt, aber nicht in K_1. Daher ist das transformierte Polynom $H(y)$ wirklich von der gewünschten Beschaffenheit; denn $a_r + Q(f)$ ist ein (nicht zu R_2 gehöriges) p-tes Radikal über K_1.

2. Fall: $n \equiv 0 \pmod{p}$.

a) Ist $P(x) = Q(x^{p^l})$ $(l \geq 1)$, so kann sich die Betrachtung auf $Q(y)$ beschränken; denn ist $Q(y)$ als reduzibel über K nachgewiesen, so ist auch $P(x)$ reduzibel[1]). Demgemäß dürfen wir (im Falle $n \equiv 0 \pmod{p}$) die Existenz eines kleinsten, zu p teilerfremden Index t annehmen, für welchen $a_t \neq 0$ in $P(x)$; es ist $2 \leq n$, $1 \leq t \leq n-1$, also $n - t - 1 \geq 0$. Man kann ferner annehmen, daß a_t nicht in K_1 liegt, weil dies andernfalls durch eine Substitution $x = cz$ (wo c zu R_1, aber nicht zu K_1 gehört) erreicht wird (vgl. 1. Fall, a).

---

[1]) Dabei ist $Q(y)$ als nicht-linear anzunehmen, weil andernfalls $P(x)$ Binom vom Grade p^l wäre. Ist der Grad m von $Q(y)$ in y nicht durch p teilbar, so kommen wir auf den 1. Fall zurück.

b) Es gehöre nun a_t, ebenso wie alle übrigen Koeffizienten von $P(x)$, zu R_1, überdies a_t nicht zu K_1. Wird $x = y + f$ gesetzt, wo f zu R_2, aber nicht zu R_1 gehört, so erhalten wir

$$P(y+f) = H(y) = y^n + \ldots + a_t y^{n-t} + (t \times a_t f + a_{t+1}^*) y^{n-t-1} + \ldots .$$

Da nämlich für die in $P(x)$ links von $a_t x^{n-t}$ stehenden Glieder (soweit sie von Null verschieden sind) der Exponent von x stets durch p teilbar ist und da $(y+f)^{p \cdot q} = (y^p + f^p)^q$ ist, so liefern besagte Glieder überhaupt keinen Beitrag zum Koeffizienten von y^{n-t}. Da ferner die Koeffizienten besagter Glieder sämtlich zu R_1 gehören und da f^p in K_1 liegt, so liefern besagte Glieder zum Koeffizienten von y^{n-t-1} — wenn überhaupt — lauter Elemente aus R_1 als Beiträge, sodaß a_{t+1}^* sicher zu R_1 gehört. Weiter ist $t \times a_t \not\equiv 0$ wegen $a_t \not\equiv 0$ und $t \not\equiv 0 \pmod{p}$, sodaß $t \times a_t f + a_{t+1}^*$ nicht zu R_1 gehört. Daher ist $H(y)$ von der gewünschten Beschaffenheit.