Vorlesung Algebra

SoSe'21, hhu
K. Halupczok

Teil III: KÖRPER

A20: Separabilität

Stichworte: separabel, (formale) Ableitung, separable Erweiterung, Fortsetzung von Körper-Einbettungen auf separable Erweiterungen, perfekter Körper, einfache Erweiterung, primitives Element, Satz vom primitiven Element.

20.1. Einleitung: Ein Polynom, das in einem ZK keine verschiedene Wurzeln hat, heißt separabel. Man kommt zu separablen Körpererweiterungen und Fragen zur Fortsetzbarkeit von Körpereinbettungen auf diese Körper. Wir zeigen damit den Satz vom primitiven Element.

20.2. Def.: $f \in K[T]$ separabel $:\Leftrightarrow$ f hat in einem ZK L unter versch. Wurzeln, d.h. $f = a \prod_{i=1}^{m} (T - x_i)$, die $x_i \in L$ paarw. versch.

20.3. Def.: Ableitung von $f = \sum_{i=0}^{m} a_i T^i \in K[T]$: $\quad f' := \sum_{i=1}^{m} i a_i T^{i-1}$

20.4. Lemma: $\forall f, g \in K[T]\ \forall a \in K$: $(f+g)' = f' + g'$, $(af)' = af'$, $(f \cdot g)' = f'g + fg'$.

Bew.: nachrechnen $\square$

20.5. Satz: $f \in K[T]$ separabel $\Leftrightarrow$ $\operatorname{ggT}(f, f') = 1$.

Bew.: Seien $x_1, \dots, x_m$ die Wurzeln von f in einem ZK L von $f|K$.

Dann: $\operatorname{ggT}(f, f') = 1 \Leftrightarrow \forall i: (T - x_i) \nmid f'$ in $L[T]$ (vgl. 20.6)

$\Leftrightarrow \forall i: f'(x_i) \neq 0$.

x_i sei Wurzel der Vielfachheit μ_i, d.h. $f = (T - x_i)^{\mu_i} f_1$, $f_1(x_i) \neq 0$.

Dann: $f' = \mu_i (T - x_i)^{\mu_i - 1} f_1 + (T - x_i)^{\mu_i} f_1'$,

also: $f'(x_i) = 0 \Leftrightarrow \mu_i - 1 \geq 1 \Leftrightarrow \mu_i > 1$.

Also: $\forall i: f'(x_i) \neq 0 \Leftrightarrow \forall i: \mu_i = 1 \Leftrightarrow f$ separabel. $\square$

20.6. Bem.: Sei $L|K$, h ein ggT von $f, g \in K[T]$ in $K[T]$, dann h auch ggT von f, g in $L[T]$.

Bew.: $\exists x, y \in K[T]: h = xf + yg$, sei $t \in L[T]$: $\exists u, v \in L[T]$ mit $f = ut$, $g = vt$.

Dann: $xut = xf = h - yg = h - yvt \Rightarrow (xu + yv)t = h \Rightarrow t | h$.

Also ist h ein ggT(f, g) in $L[T]$. $\square$

20.7. **Kor.:** Sei $f \in K[T]$ irred. Dann: f separabel $\Leftrightarrow f' \neq 0$.

Bew.: Es ist $ggT(f, f') = \begin{cases} 1, & f' \neq 0, \\ f, & f' = 0, \end{cases}$ weiter Satz 20.5. $\square$

20.8. **Kor.:** $\operatorname{Char} K = 0 \Rightarrow$ jedes $f \in K[T]$ irred., ist separabel.

Bew.: $\operatorname{Char} K = 0 \Rightarrow \deg f' = \deg f - 1$, also $f' \neq 0$. $\square$

20.9. **Def.:** Sei $L|K$, $x \in L$ alg.$|K$. x heißt separabel über K $:\Leftrightarrow \exists$ sep. $f \in K[T]: f(x) = 0$
$\Leftrightarrow$ Mipo von $x|K$ ist separabel.

20.10. **Def.:** $L|K$ heißt separable (algebraische) Erweiterung von K $:\Leftrightarrow \forall x \in L$: x ist sep.$|K$.

20.11. **Lemma:** Sei $\sigma: K \to K'$ Iso, $L = K(x_1, \dots, x_n)|K$, $E'|K'$ endl. Erw.

$$\begin{tikzcd} K(x_1,\dots,x_n) = L \arrow[r, "\bar\sigma", "\text{inj.}"'] \arrow[d, dash, "\text{sep.}"'] & E' \arrow[d, dash, "\text{norm.}"] \\ K \arrow[r, "\sigma, \text{Iso}"] & K' \end{tikzcd}$$
$f \qquad\qquad f^\sigma$

Sei $\Sigma := \{\bar\sigma: L \to E' \text{ inj.};\ \bar\sigma \restriction K = \sigma\}$. Dann gilt:

(1) $\# \Sigma \leq [L:K]$,

(2) $x_1, \dots, x_n$ sep.$|K$, $E'|K'$ normal, $\Sigma \neq \emptyset \Rightarrow \# \Sigma = [L:K]$.

Bew.: (1): VI nach n: $n = 0$: $L = K$, $\Sigma = \{\sigma\}$, $\# \Sigma = 1 \leq 1 = [L:K]$ ✓.

$n > 0$:

$$\begin{tikzcd} L \arrow[r, "\bar\sigma", "\text{inj.}"'] \arrow[d, dash] & E' \arrow[d, dash] \\ K(x_1) \arrow[r, "\sigma_i", "\text{Iso}"'] \arrow[d, dash] & K'(x_i') \arrow[d, dash] \\ K \arrow[r, "\sigma", "\text{Iso}"'] & K' \end{tikzcd}$$
$f \qquad\qquad f^\sigma$

Betr. OE $x_1 \in L$, sei $f \in K[T]$ das Mipo von $x_1|K$.

Seien $x_1', \dots, x_t'$ die versch. Wurzeln von f^σ in E' (auch: $t = 0$).

$\forall 1 \leq i \leq t\ \exists!$ Forts. $\sigma_i: K(x_1) \to E'$ von σ mit $\sigma_i(x_1) = x_i'$ (A19.6(2)).

Setze $\Sigma_i := \{\bar\sigma \in \Sigma;\ \bar\sigma(x_1) = x_i'\}$.

Dann: $\Sigma = \Sigma_1 \dot\cup \dots \dot\cup \Sigma_t \Rightarrow \# \Sigma = \sum_{i=1}^{t} \# \Sigma_i$.

IV auf Σ_i: $\# \Sigma_i \leq [L : K(x_1)]$, also $\# \Sigma \leq t \cdot [L : K(x_1)]$.

Wegen $t \leq \deg f^\sigma = \deg f = [K(x_1):K]$ folgt:

$\# \Sigma \leq [L : K(x_1)] \cdot [K(x_1) : K] = [L:K]$.

(2): Sei $\Sigma \neq \emptyset$, $E'|K'$ normal, $x_1, \dots, x_n$ sep.$|K \Rightarrow t = [K(x_1):K]$

$$\begin{tikzcd} & E' \arrow[d, dash] \\ E \arrow[r, "\tilde\sigma"] \arrow[d, dash, "\text{zk}"'] & E'' \arrow[d, dash] \\ L \arrow[d, dash, "\text{sep.}"'] & \\ K(x_1) \arrow[r, "\sigma_i"] \arrow[d, dash] & K'(x_i') \arrow[d, dash] \\ K \arrow[r, "\sigma"] & K' \end{tikzcd}$$
$f_i \qquad\qquad f_i^\sigma$
$f \qquad\qquad f^\sigma$

(denn: $\Sigma \neq \emptyset \Rightarrow f^\sigma$ hat mind. eine Wurzel in $E' \Rightarrow f^\sigma$ zerf. $|E'$ in Linearfaktoren, da E' normal)

* Für alle $1 \leq i \leq t$ ist $\Sigma_i \neq \emptyset$: (ist sep., da $f = \text{Mipo}(x_1)$ sep.)

Sei $f_i \in K[T]$ das Mipo von $x_i|K$, $f := f_1 \cdots f_n$, $E|L$ ein zk von $f|K$.

Ferner: E' enthält einen zk E'' von f^σ (denn: jedes f_i^σ hat Wurzel in E', da $\Sigma \neq \emptyset$, zerfällt also vollst. über E' (normal)).

Nach A19.11(2) $\exists$ Forts. $\tilde\sigma: E \to E''$ von $\sigma_i \Rightarrow \Sigma_i \neq \emptyset$.

* IV für Σ_i liefert: $\# \Sigma_i = [L : K(x_1)]$. Somit: $\# \Sigma = [L:K(x_1)] \cdot [K(x_1):K] = [L:K]$. $\square$

20.12. **Satz:** Sei $L = K(x_1,\dots,x_m)$ endl. Erw. von K. Dann sind äquivalent:

(1) $L|K$ separabel, (2) $x_1,\dots,x_m$ sep. $|K$.

Bew.: (1)⇒(2): ✓, (2)⇒(1): Sei $E|L$ normal über K (etwa $E = ZK$ von $f_1 \cdots f_m$, die f_i Mipo von $x_i|K$), sei $x \in L$, $f \in K[T]$ das Mipo von $x|K$.

$$\begin{tikzcd} L \arrow[r, "\bar{\sigma}_i"] \arrow[d, dash] & E \arrow[d, equal] \\ K(x) \arrow[r, "\sigma_i"] \arrow[dr, dash] & E \\ & K \arrow[u, dash] \end{tikzcd}$$

Zeige sogar: f hat $m := [K(x):K]$ versch. Wurzeln in E:

Seien $\sigma_1,\dots,\sigma_t$ die versch. Einbettungen von $K(x) \to E$.

Die versch. Wurzeln von f in E sind: $\sigma_1 x, \sigma_2 x, \dots, \sigma_t x$, mit $t \geq m$:

Für $1 \leq i \leq t$ sei $\Sigma_i = \{\bar{\sigma}_i : L \to E \text{ inj.}, \text{ Forts. von } \sigma_i\}$.

Nach Lemma 20.11: $\#\Sigma_i \leq [L:K(x)]$

$$\Rightarrow \underbrace{\#\Sigma_1 \dot\cup \dots \dot\cup \#\Sigma_t}_{=[L:K] \text{ nach Lemma 20.11}} \leq [L:K(x)] \cdot t$$

$$= [L:K(x)] \cdot [K(x):K]. \qquad \text{Somit: } t \geq [K(x):K] = m$$

Ferner: $t \leq m = [K(x):K]$ nach Lemma 20.11, also $t = m$. □

20.13. **Def:** K heißt perfekt (vollkommen) $:\Leftrightarrow$ Jede algebraische Erweiterung von K ist separabel.

20.14. **Kor.:** Körper K der Charakteristik 0 sind perfekt.

Bew.: Sei $L|K$ algebraisch, $x \in L$, f das Mipo von $x|K$.

Nach Kor. 20.8 ist f separabel, d.h. x sep. $|K$.

Also ist L separabel über K. Demnach ist K perfekt. □

20.15. **Def.:** $L|K$ einfach $:\Leftrightarrow \exists x \in L : L = K(x)$, x heißt primitives Element.

20.16. **Satz vom primitiven Element:** Jede endl. sep. Körpererw. $L|K$ ist einfach.

Bew.: Seien $\sigma_1,\dots,\sigma_m$ die versch. Einbettungen von $K(x,y) \to E$ mit $\sigma_i \restriction K = id_K$.

$$\begin{tikzcd} E \arrow[d, dash] \\ K(x,y) \arrow[r, "\text{sep.}"'] \arrow[dr, dash] & E \text{ (normal)} \\ & K \arrow[u, dash] \end{tikzcd}$$

Nach Lemma 20.11 gilt: $m = [K(x,y):K]$. $\ulcorner K(x,y) \subseteq E \lrcorner$

Die Paare $(x_1,y_1) := (\sigma_1 x, \sigma_1 y), \dots, (x_m,y_m) := (\sigma_m x, \sigma_m y)$ sind dann pwv.

$\ulcorner \sigma_1 = id_{K(x,y)} \lrcorner$

Ann.: K unendlich. $\ulcorner$ Fall: K endl. ⇒ s. Kap. A21 $\lrcorner$

Es gibt ein $c \in K$: $\overbrace{x_1 + cy_1}^{z_1}, \dots, \overbrace{x_m + cy_m}^{z_m}$ pwv. $\ulcorner$ denn: $z_i = z_j$, $i \neq j$, für höchstens ein $c \in K$, K unendl. $\Rightarrow \exists c \in K : z_1,\dots,z_m$ pwv. $\lrcorner$

$$\begin{tikzcd} K(x,y) \arrow[d, dash] \arrow[dd, bend right, dash, "m"'] \\ K(z) \arrow[d, dash, "m \leq"'] \\ K \end{tikzcd} \qquad \begin{tikzcd} K(x,y) & K(z) \arrow[l] \\ & K \arrow[u, dash] \arrow[ul, dash] \end{tikzcd}$$

Setze $z := z_1 = x_1 + cy_1$, dann $K(x,y) = K(z)$:

Lemma 20.11 ⇒ $m \leq [K(z):K]$ nach Konstruktion von z bzw. c. $\ulcorner \sigma_i|K(z)(z) = z_i \Rightarrow \sigma_1|K(z),\dots,\sigma_m|K(z)$ sind m versch. Einb. von $K(z)$ nach E über K. $\lrcorner$

Da $K(z) \subseteq K(x,y)$, folgt: $K(z) = K(x,y)$. □