

§ 19. Separable Erweiterungen und Galois-Erweiterungen

Definition (19.1)

Sei K ein Körper. Ein irreduzibles Polynom $f \in K[x]$ wird **separabel** genannt, wenn $\text{ggT}(f, f') = 1$ gilt.

Nach Proposition 18.4 ist die Separabilität von f gleichbedeutend damit, dass das irreduzible Polynom f in jedem Erweiterungskörper L von K nur **einfache Nullstellen** besitzt.

Separable Elemente und separable Körpererweiterungen

Definition (19.2)

Sei $L|K$ eine Körpererweiterung. Ein Element $\alpha \in L$ wird **separabel** über K genannt, wenn es algebraisch über K ist und sein Minimalpolynom $f \in K[x]$ separabel ist. Wir nennen die Erweiterung $L|K$ separabel, wenn jedes $\alpha \in L$ über K separabel ist.

Proposition (19.3)

Ist $L|K$ eine Körpererweiterung, $\alpha \in L$ ein über K separables Element und M ein Zwischenkörper von $L|K$, dann ist α auch separabel über M .

Anmerkung: Aus Prop. 19.3 folgt, dass für jede separable Erzw. $L|K$ und jeden Zwischenkörper M von $L|K$ auch die Erzw. $L|M$ separabel ist, genau wie bei der Eigenschaft „normal“. Im Gegensatz zu „normal“ gilt hier aber auch: $L|K$ separabel $\Rightarrow M|K$ separabel.

Bew. von Prop. 19.3: geg. Körpererw. $L|K$, $\alpha \in L$ separabel über K , M Zwischenkörper von $L|K$.
Zz. α ist separabel über M .

Sei $f = m_{\alpha,K} \in K[x]$. Dann ist f ein separables Polynom.

Sei $\tilde{L}$ ein alg. abg. Erweiterungskörper von L . Dann hat f in $\tilde{L}$ nur einfache Nullstellen.

Sei nun $g = \mu_{\alpha, m} \in M[x]$. $f \in M[x]$, $f(\alpha) = 0_K \Rightarrow g \mid f$

Da f in $\tilde{L}$ nur einfache Nullst. hat, gilt wg. $g \mid f$ dasselbe für g . Somit ist g ebenfalls separabel. $\square$

Hinreichende Bedingungen für Separabilität

Satz (19.4)

Ist K ein Körper der **Charakteristik 0**, dann ist jede algebraische Erweiterung $L|K$ separabel.

Satz (19.5)

Ist K ein **endlicher Körper**, dann ist jede algebraische Erweiterung $L|K$ separabel.

Anmerkung:

Es gibt **inseparable** (also nicht separable) algebraische Erweiterungen. Ist zum Beispiel p eine Primzahl, bezeichnet $K = \mathbb{F}_p(t)$ den **rationalen Funktionenkörper** über $\mathbb{F}_p$, und ist u eine Nullstelle von $x^p - t \in K[x]$ in einer algebraischen Erweiterung von K (die man auch mit $\sqrt[p]{t}$ bezeichnen könnte), dann ist

$K(u)|K$ eine inseparable Erweiterung.

Beweis von Satz 19.4:

geg: Körper K mit $\text{char}(K) = 0$

$L|K$ algebraische Erweiterung

z.zg: $L|K$ ist separabel

Sei $\alpha \in L$ und $f = \mu_{\alpha, K} \in K[x]$, und

Sei $n = \text{grad}(f) \in \mathbb{N}$. Dann ist

$\text{grad}(f') = n-1$ (wegen $\text{char}(K) = 0$, falsch

für $\text{char}(K) \neq 0$). denn: $\text{grad}(f) = n$,

f normiert $\Rightarrow \exists a_0, \dots, a_{n-1} \in K$ mit

$$f = x^n + \sum_{k=0}^{n-1} a_k x^k \Rightarrow f' = n \cdot x^{n-1} + \sum_{k=1}^{n-1} k a_k x^{k-1}$$

Wegen $\text{char}(K) = 0$ gilt $n \neq 0_K$ in K .

$$\rightarrow \text{grad}(f') = n - 1$$

Zu zeigen ist, dass X über K separabel ist, gleichbed. : $\text{ggT}(f, f') = 1_K$

f ist irred., $\text{ggT}(f, f') \mid f \Rightarrow \text{ggT}(f, f') = 1_K$ oder $\text{ggT}(f, f') = f$. Ang., es gilt

die zweite Gleichung. Dann folgt $f \mid f'$.

Dies ist wg $\text{grad}(f) = n$, $\text{grad}(f') = n - 1$

unmöglich. also: $\text{ggT}(f, f') = 1_K$ $\square$

Bew. von Prop. 19.5:

geg. endlicher Körper K , $q = |K| \in \mathbb{N}$
algebraische Erw. $L|K$ z.zg. $L|K$ ist separabel

Sei $\alpha \in L$ z.zg. α ist separabel über K

Sei $f = \mu_{\alpha, K}$. Zu zeigen ist, dass f ein separables
Polynom ist. Sei $d = \text{grad}(f) \Rightarrow [K(\alpha) : K] =$

$\text{grad}(f) = d \Rightarrow K(\alpha)$ ist d -dim. K -Vektorraum

$\Rightarrow |K(\alpha)| = |K|^d = q^d$. Nach § 18 sind die
Elemente von $K(\alpha)$ alles Nullstellen von $g = x^{q^d} - x$

$\in K[x]$. $\Rightarrow g(\alpha) = 0_K \Rightarrow f \mid g$

Wegen $\text{ggT}(g, g') = \text{ggT}(g, -1_K) = 1_K$ besitzt g

in jedem Eow.-btp. nur einfache Nullst., wegen
 $f' \nmid g$ gilt dasselbe für f . Also ist f ein
separables Polynom. $\square$

$\rightarrow$ In

n ,

$a_k x^{k-1}$

Beispiel für eine inseparable (= nicht separable)
algebraische Erweiterung

geg: p Primzahl, $K = \mathbb{F}_p(t)$ rationaler Fkt. Körper über $\mathbb{F}_p$
 $f = x^p - t \in K[x]$, $L|K$ Körpererweiterung, $u \in L$

Nullstelle von f Beh: $K(u)|K$ ist inseparabel

zeige: i) $f = \mu_{u,K} \Rightarrow [K(u):K] = \text{grad}(f) = p$

ii) Das Element u ist eine p -fache Nullstelle von f .

(Daraus folgt, dass f ein inseparables Polynom und u
ein über K inseparables Element ist.)

zu i) Von $\Rightarrow f$ ist normiert, u ist Nullstelle von f

noch z.zg.: f ist irreduzibel. Ang., f ist reduzibel $\Rightarrow$
 $\exists g, h \in K[x]$ mit $f = gh$, $1 \leq m, n \leq p-1$ für $m = \text{grad}(g)$,
 $n = \text{grad}(h)$ $f(u) = 0_K \Rightarrow u^p - t = 0 \Rightarrow t = u^p$
 $\Rightarrow f = x^p - t = x^p - u^p = (x - u)^p$ (*)

$\hookrightarrow \text{char } K[x] = p$

"Frobenius's Dream"

Die Pol. g und h können so gewählt werden, dass beide normiert sind
 (da f normiert ist). Dann gilt $g = (x - u)^m$, $h = (x - u)^n$. Die
 konstanten Terme von f und g sind geg. durch $(-u)^m$ bzw. $(-u)^n$ und
 müssen wegen $g, h \in K[x]$ in K liegen. Nach Def. von K
 gibt es also Polynome $r, s \in \mathbb{F}_p[t]$ mit $(-u)^m = \frac{r(t)}{s(t)} = \frac{r(u^p)}{s(u^p)}$
 $\Rightarrow s(u^p) = r(u^p) (-u)^m \Rightarrow s(u^p) - (-u)^m r(u^p) = 0$
 $\Rightarrow u$ ist Nullstelle des Polynoms $k = s(x^p) - (-x)^m r(x^p)$

Wegen $\text{grad } s(x^p) = p \cdot \text{grad } s$ und $\text{grad } (-x)^m \cdot s(x^p)$
 $= m + p \cdot \text{grad } s$ ist $k \neq 0_{\mathbb{F}_p}$ (da $p \nmid m$) $\Rightarrow u$ ist
 algebraisch über $\mathbb{F}_p \xrightarrow{t=u^p} t$ ist algebraisch über $\mathbb{F}_p$
 $\Downarrow$ da t die Unbekannte des Polynomrings $\mathbb{F}_p[t]$ ist
 Also ist f tatsächlich (red. in $K[x]$, insg. $f = \mu_{u,K}$
 zu ii) hat sich bereits gezeigt, siehe (*). □

Der Satz vom primitiven Element

Definition (19.6)

Eine Körpererweiterung $L|K$ wird **einfach** genannt, wenn ein Element $\alpha \in L$ mit $L = K(\alpha)$ existiert. In diesem Fall nennt man α ein **primitives Element** der Erweiterung.

Satz (19.7)

Jede endliche, **separable** Erweiterung $L|K$ ist einfach.

Beweis des Satzes vom primitiven Element
geg: eine endliche separable Erweiterung $L|K$
als
z.zg: $\exists x \in L$ mit $L = K(x)$

1. Schritt: Nehme an, dass die Aussage für Erweiterungen der Form $L = K(\alpha, \beta)$, α, β separabel über K bereits gezeigt wurde. Leite daraus den allgemeinen Fall her.

Zeige durch vollst. Ind. über $n \in \mathbb{N}$: Ist $L|K$ eine ^{separabel} Körpererw. und sind $\alpha_1, \dots, \alpha_n \in L$ (separabel über K) mit $L = K(\alpha_1, \dots, \alpha_n)$, dann gibt es ein $x \in L$ mit $L = K(x)$.

1. α, β
Erweite-
)
g separabel

Ind-Basis: $n=1$ N.V. gilt $L = K(\alpha_1)$ für ein $\alpha_1 \in L$

separabel über $K \Rightarrow$ nichts zu zeigen
(setze $\gamma = \alpha_1$)

Ind.-Schritt $n \rightarrow n+1$: Nach Vor. gibt es

$\alpha_1, \dots, \alpha_{n+1} \in L$, separabel über K , mit

$L = K(\alpha_1, \dots, \alpha_{n+1}) = K_1(\alpha_{n+1})$ mit

$K_1 = K(\alpha_1, \dots, \alpha_n)$. Ind.-V. $\Rightarrow \exists \gamma_1 \in K_1$

mit $K_1 = K(\gamma_1)$ $\Rightarrow L = K(\gamma_1, \alpha_{n+1})$

Laut Annahme gilt die Aussage für
zwei Erzeuger $\Rightarrow \exists \gamma \in L$ mit

$L = K(\gamma)$

=
alg
 $\Downarrow$
Also
zu li

Sei nun $L|K$ eine endliche separable Erzs.

$\Rightarrow \exists n \in \mathbb{N}$ und $\alpha_1, \dots, \alpha_n \in L$ mit $L = K(\alpha_1, \dots, \alpha_n)$

(setze $z.B. n = [L:K]$, und wähle $\alpha_1, \dots, \alpha_n$ als Basis von L als K -Vektorraum)

Aufgrund der durch Ind. bewiesenen Aussage gilt

$L = K(x)$ für ein $x \in L$.

2. Schritt: Sei $L|K$ eine separable Erzs.,

$\alpha, \beta \in L$ mit $L = K(\alpha, \beta)$. z.zg.:

$\exists x \in L$ mit $L = K(x)$. Seien $f = \mu_{\alpha, K}$

und $g = \mu_{\beta, K}$ sowie $\tilde{K}$ ein alg. abg. Erweiterungskörper von L , außerdem $m = \deg(f)$,

$n = \deg(g)$. Mit α und β sind f, g separabel

$\Rightarrow \exists \alpha_1, \dots, \alpha_m \in \tilde{K}$, alle verschieden, mit $f = \prod_{i=1}^m (x - \alpha_i)$,
 und $\beta_1, \dots, \beta_n \in \tilde{K}$, ebenfalls alle verschieden, mit
 $g = \prod_{j=1}^n (x - \beta_j)$, wobei $\alpha_1 = \alpha$ und $\beta_1 = \beta$ ist.

Betrachte für jedes $c \in K$ das Element $\gamma_c = \alpha + c\beta \in L$
 sowie das Polynom $h_c = f(\gamma_c - cx) = \prod_{i=1}^m h_{c,i}$, wobei
 $h_{c,i} = \gamma_c - cx - \alpha_i = (\alpha + c\beta) - cx - \alpha_i = (\alpha - \alpha_i) + c(\beta - x)$

Beh.: (1) $h_c(\beta) = 0$ (2) Das Element c kann so ge-
 wählt werden, dass $\beta_2, \dots, \beta_n$ keine Nullstellen von h_c sind.

Aus der Beh. folgt, dass $\text{ggT}(h_c, g)$ für solch ein c

gleich $x - \beta$ ist. Setzt man $M_c = K(\gamma_c)$, dann sind g und h_c in $M_c[x] \Rightarrow x - \beta = \text{ggT}(g, h_c) \in M_c[x] \Rightarrow \beta \in M_c \Rightarrow \alpha = \gamma_c + c\beta \in M_c \Rightarrow K(\alpha, \beta) \subseteq M_c = K(\gamma_c)$. Da umgekehrt $\gamma_c \in K(\alpha, \beta)$ gilt, folgt $K(\alpha, \beta) = K(\gamma_c)$.

zu (1) Es gilt $h_{c,1}(\beta) = (x - \alpha_1) + c(\beta - \beta) = 0$
 Wegen $h_{c,1} \mid h_c$ folgt $h_c(\beta) = 0$ $\uparrow \alpha_1 = x$

zu (2) (für den Fall, dass K unendlich ist) $h_c = \prod_{i=1}^m h_{c,i}$

Für $2 \leq j \leq n$ gilt die Äquivalenz $h_c(\beta_j) \neq 0 \Leftrightarrow$

$h_{c,i}(\beta_j) \neq 0$ für $1 \leq i \leq m \Leftrightarrow (x - \alpha_i) + c(\beta - \beta_j) \neq 0$

für $1 \leq i \leq m$. $\Leftrightarrow c \neq \frac{\alpha_i - x}{\beta - \beta_j}$ für $1 \leq i \leq m$. Da K unendlich ist, existiert ein c mit $c \neq \frac{\alpha_i - x}{\beta - \beta_j}$ für $1 \leq i \leq m, 2 \leq j \leq n$.

Beweis von Satz 19.7 (Abschluss)

Im Fall, dass K ein **endlicher** Körper ist, kann die Existenz eines Elements $\gamma \in L$ mit $L = K(\gamma)$ folgendermaßen gezeigt werden: Weil α und β beide algebraisch über K sind, ist $L|K$ mit $L = K(\alpha, \beta)$ eine endliche Erweiterung, und folglich ist mit K auch L ein endlicher Körper. Nach Satz 14.13 ist die multiplikative Gruppe $L^\times$ von L eine **zyklische** Gruppe. Es existiert also ein $\gamma \in L^\times$ mit

$$L^\times = \langle \gamma \rangle = \{ \gamma^m \mid m \in \mathbb{Z} \}.$$

Dieses Element erfüllt dann offenbar auch die Gleichung $L = K(\gamma)$.