Definition (19.1)

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

Beweis von Proposition 19.3

geg: Körpererweiterung $L|K$, M Zwischenkrp. von $L|K$
$\alpha \in L$, separabel über K z.zg: α ist separabel über M

Sei $f = \mu_{\alpha,K} \in K[x]$ und $g = \mu_{\alpha,M} \in M[x]$
α sep. über K $\Rightarrow$ f ist separables Polynom $\Rightarrow$ f hat
keine mehrfache Nullstelle in einer Erweiterung von K (*)
$f \in M[x]$, $f(\alpha) = 0 \rightarrow g \mid f$ Weil (*) für f gilt,
gilt sie auch für g $\Rightarrow$ g ist separables Pol in $M[x]$
$\Rightarrow$ α ist separabel über M. $\square$

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

$$K(u)|K \quad \text{eine inseparable Erweiterung.}$$

Beispiel für eine inseparable Erweiterung

geg: Primzahl p, $K = \mathbb{F}_p(t)$ rationaler Funktionenkörper über $\mathbb{F}_p$, $L|K$ Erweiterung, $u \in L$ Nullstelle von $f = x^p - t \in K[x]$

<u>Beh.</u> $K(u)|K$ ist inseparabel

zeige: u ist nicht separabel über K, d.h. $g = \mu_{u,K} \in K[x]$ ist kein separables Polynom

Es gilt $f(u) = \bar{0} \Rightarrow u^p - t = \bar{0} \Rightarrow u^p = t$

$\Rightarrow f = x^p - u^p = (x-u)^p$

„Freshman's Dream" §18

d.h. u ist p-fache Nullstelle von f

<u>Beh.</u>: $g = f$ (Daraus folgt, dass g kein separables Polynom in $K[x]$ ist.)

$f(u) = \bar{0}$, $g = \mu_{u,K} \Rightarrow g \mid f$. Ang. g ist ein echter Teiler von f. Dann gilt $g = (x-u)^m$ für ein $m \in \{1, \ldots, p-1\}$. Der konstante Term von g, das Element $(-1)^m u^m$, ist in K enthalten (wg. $g \in K[x]$). Nach Def. von $K = \mathbb{F}_p(t)$ gibt es Pol. $h, k \in \mathbb{F}_p[x]$ mit

$$(-1)^m u^m = \frac{h(t)}{k(t)} = \frac{h(u^p)}{k(u^p)} \Rightarrow (-1)^m u^m \cdot k(u^p) = h(u^p)$$

$\Rightarrow u$ ist Nullstelle von $F = (-1) x^m k(x^p) - h(x^p) \in \mathbb{F}_p[x]$. Es ist $F \neq \bar{0}$, da der Grad von $h(x^p)$, im Gegensatz zum Grad von $(-1)^m x^m k(x^p)$, durch p teilbar ist.

$F \neq \bar{0}$, $F \in \mathbb{F}_p[x]$, $F(u) = \bar{0} \Rightarrow u$ ist algebraisch über $\mathbb{F}_p$

$\Rightarrow t = u^p$ ist algebraisch über $\mathbb{F}_p \Rightarrow$ Es gibt ein Pol

$G \in \mathbb{F}_p[x]$ mit $G(t) = \bar{0}$. $\lightning$ da $G(t)$ aus G nur durch

Umbenennung der Variablen entsteht ($x \mapsto t$).

$\square$

also: $m = p$, $g = (x-u)^p = f$.

Beweis von Satz 19.4

geg: alg. Körpererw. $L|K$ mit $\mathrm{char}(K) = 0$

zzg: $L|K$ ist separabel

Sei $\alpha \in L$. zzg: α ist separabel über K. Sei $f = \mu_{\alpha,K}$.

zzg: f ist separables Polynom in $K[x]$, d.h. $\mathrm{ggT}(f, f') = 1_K$.

Sei $n = \mathrm{grad}(f)$. Dann gilt $\mathrm{grad}(f') = n-1$ (denn: Sei $f = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, mit $a_0, \ldots, a_{n-1} \in K$. $\Rightarrow f' = n x^{n-1} + \sum_{k=1}^{n-1} k a_k x^{k-1}$ und $n \neq 0_K$ wg. $\mathrm{char}(K) = 0$.) Sei $h = \mathrm{ggT}(f, f')$.

$h \mid f$, f ist irred. $\Rightarrow h = 1_K$ oder $h = f$ (bis auf eine Konstante in K^*). $h \mid f' \Rightarrow \mathrm{grad}(h) \leq n-1 \Rightarrow h = 1_K$. $\square$

Beweis von Satz 19.5

geg.: K endlicher Körper

$L|K$ algebraische Erweiterung

z.zg.: $L|K$ ist separabel

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

Da α algebraisch über K ist, ist $K(\alpha)|K$ eine <u>endliche</u> Erweiterung. Sei $q = |K|$, $r = [K(\alpha):K]$. $\Rightarrow$ $K(\alpha)$ ist r-dim. K-Vektorraum und $|K(\alpha)| = q^r$. In § 18 wurde gezeigt, dass die Elemente des endl. Körpers $K(\alpha)$ genau die q^n verschiedenen Nullstellen des Polynoms $f = X^{q^n} - X \in K[X]$ sind. Sei $g = \mu_{\alpha,K}$. $f(\alpha) = 0_K \Rightarrow g \mid f$. Da f (weder in $K(\alpha)$ noch eines anderen Erweiterung von K) mehrfache Nullstellen besitzt, gilt dasselbe für g. $\Rightarrow g$ ist ein separables Pol. in $K[X]$. $\Rightarrow \alpha$ ist separabel über dem Körper K $\square$

d.

Be

$f(u$

echt

$m \in$

$(-1)^m$

von K

$(-1)^m$

$\Rightarrow u$

$\in \mathbb{F}_p$

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 eine primitives Element der Erweiterung.

Satz (19.7)

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

Beweis von Satz 19.7

geg. endliche separable Erweiterung $L|K$

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

1. Fall: K ist endlich

Mit K ist dann auch L endlich. Daraus folgt, dass $L^\times$ eine endliche zyklische Gruppe ist, d.h. es gibt ein $\gamma \in L^\times$ mit

$L^\times = \langle \gamma \rangle = \{ \gamma^m \mid m \in \mathbb{Z} \} \Rightarrow L = K(\gamma)$

2. Fall: K ist unendlich

Da $L|K$ endlich ist, gibt es ein $r \in \mathbb{N}$ und $\alpha_1, \dots, \alpha_r \in L$

mit $L = K(\alpha_1, \dots, \alpha_r)$. Es genügt also, durch vollst. Ind. über r zu zeigen: Ist K ein unendl. Körper, $L|K$ eine Erw., $r \in \mathbb{N}$ und sind $\alpha_1, \dots, \alpha_r \in L$ mit $L = K(\alpha_1, \dots, \alpha_r)$, dann existiert ein $\alpha \in L$ mit $L = K(\alpha)$

<u>Ind.-Anf.</u> $r = 1$ nichts zu zeigen, setze $\alpha = \alpha_1$.

<u>Ind-schritt</u>: Sei $r \in \mathbb{N}$, setze die Aussage für r voraus.

Seien $L|K$ wie oben, $\alpha_1, \dots, \alpha_{r+1} \in L$ mit $L = K(\alpha_1, \dots, \alpha_r, \alpha_{r+1})$

Ind.-V. $\Rightarrow \exists\, \alpha \in L$ mit $K(\alpha) = K(\alpha_1, \dots, \alpha_r)$

Setzen wir $\beta = \alpha_{r+1}$, dann folgt $L = K(\alpha, \beta)$.

zu zeigen bleibt also: $\exists\, \gamma \in L$ mit $K(\gamma) = K(\alpha, \beta)$

Seien $f, g \in K[x]$ geg. durch $f = \mu_{\alpha,K}$, $g = \mu_{\beta,K}$, außerdem $m = [K(\alpha):K] = \text{grad}(f)$, $n = [K(\beta):K] = \text{grad}(g)$

Sei $\tilde{K}$ ein alg. Abschluss von K. Es seien $\alpha_1, \dots, \alpha_m$ die Nullst. von f in $\tilde{K}$, $\beta_1, \dots, \beta_n$ die Nullst. von g in $\tilde{K}$, wobei $\alpha_1 = \alpha$, $\beta_1 = \beta$.

$\Longrightarrow f = \prod_{i=1}^{m} (x - \alpha_i)$, $g = \prod_{j=1}^{n} (x - \beta_j)$. Weil α und β separabel über K sind, sind die m Elemente α_i alle verschieden, und ebenso die n Elemente β_j.

Für jedes $c \in K$ setze $\gamma_c = \alpha + c\beta$ und $h_c = f(\gamma_c - cx) = \prod_{i=1}^{m} h_{c,i}$ mit $h_{c,i} = (\gamma_c - cx) - \alpha_i = \gamma_c - (\alpha_i + cx)$ für $1 \le i \le m$. Setzt man $M_c = K(\gamma_c)$, dann liegt $f(\gamma_c - cx) \in M_c[x]$

Betrachte nun $\operatorname{ggT}(h_c, g) \in M_c[x]$.

Es gilt $h_c(\beta_1) = h_c(\beta) = f(\gamma_c - c\beta) = f(\alpha + c\beta - c\beta) = f(\alpha) = 0_K$, d.h. β_1 ist Nullstelle von h_c.

<u>Beh.</u>: Die Konstante $c \in K$ kann so gewählt werden, dass keines der Elemente $\beta_2, \dots, \beta_n$ eine Nullstelle von h_c ist. (Dann gilt $\operatorname{ggT}(h_c, g) = x - \beta_1 = x - \beta$,

$=$

$) - \alpha_i$

am

$]$

t werden.

ullstelle

$= \alpha - \beta.$

und wir erhalten $\beta \in M_c$.)

Sei $c \in K$. Für $2 \leq j \leq n$ gilt jeweils die Äquivalenz $h_c(\beta_j) = 0_K \iff \exists\, i \in \{1, \dots, m\}$ mit $h_{c,i}(\beta_j) = 0_K \iff \exists\, i \in \{1, \dots, m\}$ mit $\gamma_c - (\alpha_i + c\beta_j) = 0_K \iff \exists\, i : \gamma_c = \alpha_i + c\beta_j$

$\iff \exists\, i : \alpha + c\beta = \alpha_i + c\beta_j \implies \exists\, i :$

$c(\beta_j - \beta) = \alpha - \alpha_i \iff \exists\, i : c = \dfrac{\alpha - \alpha_i}{\beta_j - \beta}$

Wählen wir also $c \in K$ so, dass $c \neq \dfrac{\alpha - \alpha_i}{\beta_j - \beta}$ für $1 \leq i \leq m$ und $2 \leq j \leq n$ gilt, dann ist keines der Elemente $\beta_2, \dots, \beta_n$ eine Nullstelle von h_c. Dies ist möglich, weil K unendlich ist. $(\Rightarrow$ Beh.$)$

Der Separabilitätsgrad einer Erweiterung

Satz (19.8)

Sei $L|K$ eine endliche Erweiterung und $\tilde{K}$ ein algebraisch abgeschlossener Erweiterungskörper von L. Dann gilt

$$|\mathrm{Hom}_K(L, \tilde{K})| \le [L : K]$$

mit Gleichheit genau dann, wenn die Erweiterung $L|K$ separabel ist.

Definition (19.9)

Sei $L|K$ eine endliche Erweiterung und $\tilde{K}$ ein algebraisch abgeschlossener Erweiterungskörper von L. Dann nennt man

$$[L : K]_{\mathrm{sep}} \quad = \quad |\mathrm{Hom}_K(L, \tilde{K})|$$

den Separabilitätsgrad der Erweiterung $L|K$.

Beweis von Satz 19.8, zunächst nur „$\Rightarrow$"

geg.: endl. Körpererw. $L|K$, $\check{K}$ ein alg. abg. Erweiterungskörper

Zeige „$\Rightarrow$" durch Kontraposition, d.h. wir zeigen:
Ist $L|K$ inseparabel, dann gilt $|\mathrm{Hom}_K(L, \check{K})| < [L:K]$.
Dabei nehmen wir an, dass „$\Leftarrow$" und die „$\leq$"-Aussage schon gezeigt wurden (machen wir nächste Stunde).

$L|K$ inseparabel $\Rightarrow$ $\exists\, \alpha \in L$, das nicht separabel über K ist,
d.h. $f = \mu_{\alpha,K}$ ist kein separables Polynom in $K[x]$.

d.h. $f = \mu_{\alpha,K}$ ist kein separables Polynom in $K[x]$.

Sei $n = \mathrm{grad}(f) = [K(\alpha):K]$, und seien $\alpha_1, \dots, \alpha_m$ die Nullstellen von f in $\tilde{K}$. f nicht separabel $\Rightarrow m < n$.

Satz 16.4 $\Rightarrow$ Es gibt genau m K-Hom. $K(\alpha) \to \tilde{K}$. Bezeichne diese mit $\psi_1, \dots, \psi_m$. Setze $r = [L:K(\alpha)] = \frac{[L:K]}{\underbrace{[K(\alpha):K]}_{\text{grad} f}} = \frac{[L:K]}{n}$.

Annahme $\Rightarrow$ Jedes ψ_i besitzt höchstens r Fortsetzungen auf den Körper L. Da jedes $\varphi \in \mathrm{Hom}_K(L, \tilde{K})$ durch Fortsetzung eines ψ_i zu Stande kommt, folgt $|\mathrm{Hom}_K(L, \tilde{K})| \leq m \cdot r = m \cdot \frac{[L:K]}{n} = \frac{m}{n} \cdot [L:K]$

$\underbrace{<}_{m<n} [L:K]$. $\square$