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.

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

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

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.

Der Separabilitätsgrad einer Erweiterung

Satz (19.8)

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

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

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 $L|K$.

$[L:K]$, so dass genau s

Beweis von Satz 19.8

geg.: endl. Körpererw. $L|K$, $\tilde{K}$ alg. abg. Erw.-körper von K

Zzg.: $|\mathrm{Hom}_K(L,\tilde{K})| \leq [L:K]$ mit „$=$"
genau dann, wenn $L|K$ separabel ist

Bew. von „$\Leftarrow$" und der Ungleichung

Zeige allgemeiner: geg. ein Körperhom. $\phi: K \to \tilde{K}$,
$L|K$ endl. Erw., dann gibt es $\leq [L:K]$ verschiedene
Fortsetzungen von ϕ auf L, und genau $[L:K]$
Fortsetzungen, falls $L|K$ separabel ist

Beweis durch vollst. Ind. über $n = [L:K]$:

Ind-Anf. $n=1$ $[L:K] = 1 \Rightarrow L = K$ In diesem Fall gibt es genau eine Forts. von ϕ auf L, nämlich ϕ selbst.

Ind-schritt: Sei $n \in \mathbb{N}$, $L|K$ eine Erw. von Grad $n+1$, setze die Aussage für Erweiterungen von Grad $\leq n$ voraus.
Sei $\alpha_1, \dots, \alpha_r$ ein minimales Esz.-system von $L|K$, d.h. keine echte Teilmenge von $\{\alpha_1, \dots, \alpha_r\}$ erzeugt den Erw.-körper L von K. Setze $M = K(\alpha_1, \dots, \alpha_{r-1})$, $\alpha = \alpha_r$.
$\Rightarrow L = M(\alpha)$ und $[M:K] \leq n$ auf Grund der Minimalität
Ind-V. $\Rightarrow$ Es gibt ein $s \leq [M:K]$, so dass genau s

Fortsetzungen von ϕ auf M existieren.
Bezeichne diese mit $\psi_1, \ldots, \psi_s$. Sei
$f = M_{\alpha, M}$. Nach Folgerung 16.4 aus
dem Fortsetzungssatz gilt es für
$1 \leq j \leq s$ jeweils genauso viele Fort-
setzungen von ψ_j auf $L = M(\alpha)$,
wie das Polynom $\phi(f)$ Nullstellen in
$\hat{K}$ besitzt. Die Anzahl dieser Nullst
ist beschränkt durch $\operatorname{grad} \phi(f) = \operatorname{grad}(f)$
$\operatorname{grad} M_{\alpha, M} = [M(\alpha) : M] = [L : M]$

Umgekehrt ist jede Fortsetzung $\tilde{\varphi}$ von φ auf L die Fortsetzung von einem der Hom. χ_σ. Daraus folgt insgesamt, dass die Anz. der Forts. von φ auf L durch $s \cdot [L:M] \leq [M:K] \cdot [L:M] = [L:K]$ (↑ Gradformel) beschränkt ist.

Setze nun voraus, dass $L|K$ separabel ist. Dann ist auch $M|K$ separabel. Auf Grund der Ind.-V. gilt dann $s = [M:K]$. Mit $L|K$ ist auch $L|M$ separabel, insb. ist α über M separabel und $f = \mu_{\alpha,M}$ ein

separables Polynom; ebenso $\phi(f)$

$\tilde{K}$ alg. abgeschlossen, $\phi(f)$ separabel $\Rightarrow$ Die Anzahl der Nullstellen von $\phi(f)$ in $\tilde{K}$ ist gleich $\operatorname{grad}\phi(f)$ $= \operatorname{grad}(f) = [M(\alpha) : M] = [L : M]$.

Insgesamt gibt es dann genau $s \cdot [L : M] = [M : K] \cdot [L : M] = [L : K]$ Fortsetzungen von ϕ auf L.

Zeige noch: Ist $L|K$ nicht separabel, dann gilt $|\mathrm{Hom}_K(L, \tilde{K})| < [L : K]$.

$L|K$ nicht separabel $\Rightarrow \exists \alpha \in L$, das nicht separabel

über K ist. Es gibt dann $\alpha \in L \setminus K \Rightarrow$

$$[K(\alpha):K] > 1 \Rightarrow [L:K(\alpha)] = \frac{[L:K]}{[K(\alpha):K]} < [L:K]$$

$\leq$ grad f.

Die Anzahl der K-Hom. $K(\alpha) \to \tilde{K}$ ist (wieder nach Folg. 16.4) gleich der Anzahl der Nullstellen von $f = \mu_{\alpha,K}$ in $\tilde{K}$. α nicht sep. $\Rightarrow$ f ist kein separables Polynom. $\Rightarrow$ Die Anz. der Nullstellen ist kleiner als $\text{grad}(f) = [K(\alpha):K]$. Für jede Fort. $\psi: K(\alpha) \to \tilde{K}$ von ϕ gibt es höchstens $[L:K(\alpha)]$ Möglichkeiten, diese weiter auf L fortzusetzen (siehe oben). Insgesamt gibt es also dreimal weniger als $[K(\alpha):K] \cdot [L:K(\alpha)]$ K-Homomorphismen $L \to \tilde{K}$. □

Das Minimalpolynom über einem Zwischenkörper

Lemma (19.10)

Sei $L|K$ eine einfache algebraische Erweiterung, also $L = K(\alpha)$ für ein $\alpha \in L$. Sei M ein Zwischenkörper von $L|K$ und

$$f \quad = \quad \mu_{\alpha,M} \quad = \quad x^n + \sum_{i=0}^{n-1} a_i x^i \quad \in M[x]$$

das Min.-polynom von α über M. Dann gilt $M = K(a_0, ..., a_{n-1})$.

Beweis von Lemma 19.10:

geg.: endliche Erw. $L|K$, $\alpha \in L$ mit $L = K(\alpha)$

Sei M ein Zwischenkörper von $L|K$ und $f = \mu_{\alpha, M} \in M[x]$.

Schreibe $f = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$ mit $a_0, \dots, a_{n-1} \in M$

(wobei $n = [M(\alpha) : M] = [L : M]$)

Beh.: $M = M_0$, wobei $M_0 = K(a_0, \dots, a_{n-1})$

„$\supseteq$" ist offensichtlich, da $a_0, \dots, a_{n-1} \in M \Rightarrow M_0 = K(a_0, \dots, a_{n-1}) \subseteq M$

„$=$" Es gilt $f \in M_0[x]$, da $a_0, \dots, a_{n-1} \in M_0$. Daraus folgt

$f = \mu_{\alpha, M_0}$, denn: f ist normiert, hat α als Nullstelle,

$f \in M_0[x] \Rightarrow \mu_{\alpha, M_0} \mid f$, außerdem: $\operatorname{grad}(\mu_{\alpha, M_0}) =$

$[M_0(\alpha) : M_0] = [L : M_0] \overset{M_0 \subseteq M}{\geq} [L : M] = [M(\alpha) : M] =$

grad f unzg. $\mu_{\alpha, M_0} \mid f$. $\operatorname{grad}(\mu_{\alpha, M_0}) \geq \operatorname{grad}(f) \Rightarrow f = \mu_{\alpha, M_0}$

$\Rightarrow [L : M_0] = [M_0(\alpha) : M] = \operatorname{grad}(f) = [M(\alpha) : M] = [L : M]$

$\Rightarrow [M_0 : K] = \frac{[L : K]}{[L : M_0]} = \frac{[L : K]}{[L : M]} = [M : K]$.

($[L : M_0]$ = grad f)

$M_0 \subseteq M$

$\Rightarrow M_0 = M$

$\square$

Charakterisierung der einfachen Erweiterungen

Satz (19.11)

Eine endliche Erweiterung $L|K$ besitzt genau dann nur endlich viele Zwischenkörper, wenn sie einfach ist.

Folgerung (19.12)

Jede endliche, separable Erweiterung $L|K$ besitzt nur endlich viele Zwischenkörper.

Bew. von Satz 19.11

geg: endl. Erweiterung $L|K$

Beh.: $L|K$ ist einfach $\Longleftrightarrow$ Es gibt in $L|K$ nur endlich viele Zwischenkörper.

(d.h. $\exists \alpha \in L$ mit $L = K(\alpha)$)

1. Fall: K ist endlich

K endlich, $L|K$ endlich $\Rightarrow$ L endlich

Damit hat L nur endl. viele Teilmengen, und somit kann $L|K$ auch nur endlich viele Zwischenkörper haben.

außerdem: Da L endlich ist, ist $L^\times$ eine zykli-

sche Gruppe, d.h. es gibt ein $\alpha \in L^\times$ mit $L^\times = \{\alpha^n \mid n \in \mathbb{Z}\}$. Für dieses α gilt dann auch $L = K(\alpha)$. Insgesamt sind also beide Seiten der Äquivalenz wahr, damit auch die Äquivalenz selbst.

2. Fall: K ist unendlich

„$\Rightarrow$" Vor.: $\exists \alpha \in L$ mit $L = K(\alpha)$. Sei $f = \mu_{\alpha, K}$. bekannt: Ist M ein Zwischenkörper ist, dann ist $g = \mu_{\alpha, M}$ ein normierter Teiler von f. Auf Grund von Lemma 19.10 kann der Zwischenkörper M aus dem Teiler $g \mid f$ rekonstruiert werden (nämlich durch Adjunktion der Koeffizienten von g an K).

Also ist die Zuordnung

$\{$ Zwischenkörper von $L|K\} \xrightarrow{(*)} \{$ normierte Teiler von $f\}$

$$M \longmapsto M_{K,M}$$

eine injektive Abbildung. Jedes Polynom hat nur endlich viele normierte Teiler in $L[x]$ (höchstens alle möglichen Produkte von normierten Linearfaktoren der Form $x-\gamma$, $\gamma \in L$ Nullstelle von f)

Da also die Menge auf rechten Seite von $(*)$ endlich ist, muss auch die linke Seite endlich sein.

„$\Leftarrow$" Vor.: $L|K$ hat nur endlich viele Zwischenkörper z.Zg.: $\exists \gamma \in L$ mit $L = K(\gamma)$

Wie beim Beweis des Satzes vom primitiven Element kann der Beweis auf den Fall zurückgeführt werden, dass es $\alpha, \beta \in L$ mit $L = K(\alpha, \beta)$ gibt.

z.Zg. also: $\exists \gamma \in L$ mit $L = K(\alpha, \beta)$

Betrachte für jedes $c \in K$ das Element $\gamma_c = \alpha + c\beta$.

Dann ist $K(\gamma_c)$ jeweils ein Zwischenkörper von L/K.

K ist unendlich, es gibt nur endl viele Zwischenkörper.

$\Rightarrow \exists c, d \in K$ mit $c \neq d$ mit $K(\gamma_c) = K(\gamma_d)$.

$\gamma_c, \gamma_d \in K(\gamma_c) \Rightarrow \alpha + c\beta, \alpha + d\beta \in K(\gamma_c) \Rightarrow$

$(\alpha + c\beta) - (\alpha + d\beta) = (c-d)\beta \in K(\gamma_c)$ $\overset{c \neq d}{\Rightarrow}$ $c - d \in K^\times$

$\beta \in K(\gamma_c)$, $\alpha = \gamma_c - c\beta \in K(\gamma_c)$

also: $\alpha, \beta \in K(\gamma_c) \Rightarrow L = K(\alpha, \beta) \subseteq K(\gamma_c)$

Umgekehrt gilt offenbar $K(\gamma_c) \subseteq L$, insgesamt also

$L = K(\gamma)$.

□

Definition der Galois-Erweiterungen

Definition (19.13)

Eine Körpererweiterung $L|K$ wird Galois-Erweiterung genannt, wenn sie normal und separabel ist. Die Gruppe

$$\mathrm{Gal}(L|K) \quad = \quad \mathrm{Aut}_K(L)$$

wird dann die Galoisgruppe der Erweiterung $L|K$ genannt.

Ist M ein Zwischenkörper einer galois'schen Erweiterung $L|K$, dann ist auch $L|M$ galois'sch.

Charakterisierung der Galois-Erweiterungen

Satz (19.14)

Eine endliche Körpererweiterung $L|K$ ist genau dann galois'sch, wenn

$$[L : K] \quad = \quad |\mathrm{Aut}_K(L)|$$

gilt. Insbesondere ist für jede endliche Galois-Erweiterung $L|K$ also die Gleichung $|\mathrm{Gal}(L|K)| = [L : K]$ erfüllt.

Der Beweis von Satz 19.14, d.h.

$$L|K \text{ galoissch} \iff [L:K] = |\mathrm{Aut}_K(L)|$$

für jede endl. Erweiterung erhält man durch Kombination der folgenden beiden Ergebnisse.

(i) $L|K$ normal $\iff \mathrm{Hom}_K(L, \tilde{K}) = \mathrm{Aut}_K(L)$

wobei $\tilde{K} \supseteq L$ alg. abg. Erweiterungskp.

(ii) $L|K$ separabel $\iff |\mathrm{Hom}_K(L, \tilde{K})| = [L:K]$

$$\| \\ [L:K]_{sep}$$