Normale Erweiterungen

Definition (17.13)

Eine algebraische Körpererweiterung $L|K$ heißt normal, wenn folgende Bedingung erfüllt ist: Ist $f \in K[x]$ ein irreduzibles Polynom, das in L eine Nullstelle besitzt, dann zerfällt f über L in Linearfaktoren.

Proposition (17.14)

Sei $L|K$ eine Körpererweiterung vom Grad 2. Dann ist $L|K$ normal.

Charakterisierung der normalen Erweiterungen

Satz (17.15)

Sei K ein Körper, und seien $\tilde{K} \supseteq L \supseteq K$ Erweiterungen von K, wobei $L|K$ endlich und $\tilde{K}$ algebraisch abgeschlossen ist. Dann sind folgende Aussagen äquivalent:

(i) $L|K$ ist normal.

(ii) Es gibt ein nicht-konstantes Polynom $f \in K[x]$, so dass L der Zerfällungskörper von f über K ist.

(iii) Es gilt $\mathrm{Hom}_K(L, \tilde{K}) = \mathrm{Aut}_K(L)$.

Beweis von Satz 17.15

geg: endl. Erw. $L|K$, $\tilde{K} \supseteq L$ alg. abg. Erweiterungskörp.

z.zg: Äquivalenz der drei Aussagen

(i) $L|K$ ist normal (ii) L ist Zerf.körp. eines $f \in K[x]$ über K

(iii) $\mathrm{Hom}_K(L, \tilde{K}) = \mathrm{Aut}_K(L)$

„(i) $\Rightarrow$ (ii)" $L|K$ endlich $\Rightarrow \exists \alpha_1, \dots, \alpha_r \in L$ mit $L = K(\alpha_1, \dots, \alpha_r)$

Sei $f_i = \mu_{\alpha_i, K}$ für $1 \le i \le r$ und $f = \prod_{i=1}^{r} f_i$.

Beh.: L ist Zerf.körp. von f über K

Da jedes f_i jeweils die Nullst. α_i in L besitzt und (als

Min.-pol.) in $K[x]$. Folgt aus der Vor., dass $L|K$ normal ist, dass jedes f_i über L in Linearfaktoren zerfällt. Damit zerfällt auch f über L in Linearfaktoren. Da $L|K$ bereits von $\alpha_1, \dots, \alpha_r$ erzeugt wird, wird sie erst recht von der Gesamtheit der Nullst. des Polynoms f in L erzeugt.

„(ii) $\Rightarrow$ (iii)" z.Zg. $\mathrm{Hom}_K(L, \tilde{K}) = \mathrm{Aut}_K(L)$ Die Inklusion „$\supseteq$" ist offensichtlich, weil jedes $\sigma: L \to L$ in $\mathrm{Aut}_K(L)$ wegen $L \subseteq \tilde{K}$ auch als K-Hom. $L \to \tilde{K}$ betrachtet werden kann.

„$\subseteq$" Sei $\sigma \in \mathrm{Hom}_K(L, \tilde{K})$. Es genügt zu zeigen, dass $\sigma(L) \subseteq L$ abbildet, denn dann ist σ ein Element von $\mathrm{Hom}_K(L, L)$, und nach § 16 gilt $\mathrm{Hom}_K(L, L) = \mathrm{Aut}_K(L)$, weil $L|K$ eine algebraische Erweiterung ist.

Auf Grund der Vor. (ii) gilt $L = K(N)$, wobei N die Menge der Nullstellen eines Polynoms $f \in K[x]$ bezeichnet. Wegen $L = K(N)$ folgt die Inklusion $\sigma(L) \subseteq L$ bereits aus $\sigma(N) \subseteq L$ denn es ist $\sigma(L) = \sigma(K(N)) = \sigma(K)(\sigma(N))$ $\overset{\S 16}{=} K(\sigma(N))$. Da σ ein K-Hom. ist, wird $\overset{\sigma\ K\text{-Hom}}{=}$ jede Nullst. von $f \in K[x]$ aus L wieder auf eine Nullst. von f abgebildet. Somit gilt tatsächlich $\sigma(N) \subseteq N \subseteq L$.

„(iii) $\Rightarrow$ (i)" Sei $f \in K[x]$ ein irreduzibles Poly-

kann, dass in L eine Nullstelle α besitzt. z.zg.: f zerfällt über L in Linearfaktoren. Da $\tilde{K}$ alg abgeschlossen ist, zerfällt f jedenfalls über $\tilde{K}$ in Linearfaktoren. Es genügt somit zu zeigen, dass jede Nullst. von f in $\tilde{K}$ bereits in L liegt. Sei also $\beta \in \tilde{K}$ eine Nullst. von f, z.zg. $\beta \in L$.

Da f irreduzibel und α, β Nullstellen von f sind, existiert ein K-Hom. $\phi : K(\alpha) \to \tilde{K}$ mit $\phi(\alpha) = \beta$. Da $\tilde{K}$ algebraisch abgeschl. ist, kann ϕ zu einem K-Hom. $\psi : L \to \tilde{K}$ fortgesetzt werden. $\psi \in \mathrm{Hom}_K(L, \tilde{K}) \overset{\text{Vor. (iii)}}{\Rightarrow} \psi \in \mathrm{Aut}_K(L) \Rightarrow \beta = \psi(\alpha) \in L$. $\square$

Die Konjugierten eines Elements

Definition (17.16)

Sei $L|K$ eine normale Erweiterung und $\alpha \in L$. Dann werden die Nullstellen des Minimalpolynoms $\mu_{\alpha,K}$ in L die Konjugierten des Element α über K genannt.

alternative Charakterisierung:

Sei $L|K$ eine normale Erweiterung. Zwei Elemente α, β sind genau dann zueinander konjugiert (also β ein Konjugiertes von α), wenn ein $\sigma \in \mathrm{Aut}_K(L)$ mit $\sigma(\alpha) = \beta$ existiert.

Teilerweiterungen normaler Erweiterungen

Proposition (17.17)

Ist $L|K$ eine normale Erweiterung und M ein Zwischenkörper von $L|K$, dann ist auch die Erweiterung $L|M$ normal.

Hinweis:

Die Teilerweiterung $M|K$ der normalen Erweiterung $L|K$ ist im Allgemeinen nicht normal.

Gegenbeispiel:

$K = \mathbb{Q}$, $M = \mathbb{Q}(\sqrt[3]{2})$, $L = \mathbb{Q}(\sqrt[3]{2}, \zeta)$ mit $\zeta = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}$

Beweis von Proposition 17.17:

geg: normale Erweiterung $L|K$

M Zwischenkörper von $L|K$

zzg: $L|M$ ist normal

Sei $f \in M[x]$ ein (über M) irreduzibles Polynom, dass in L eine Nullstelle α besitzt

zzg: f zerfällt über L in Linearfaktoren

Auf Grund der Voraussetzungen gilt $f = c\, \mu_{\alpha, M}$ für ein $c \in M^\times$. Betrachte $g = \mu_{\alpha, K} \in K[x]$.

Es gilt $g \in M[x]$ und $g(\alpha) = 0$ $\Rightarrow$

für ein $c \in M^*$ Betrachte $g = M_{\alpha,K} \in K[x]$

$M_{\alpha,M} \mid g \Rightarrow f \mid g$ Weil $L|K$ normal ist und $g \in K[x]$ irreduzibel ist, mit $\alpha \in L$ als Nullstelle, zerfällt g über L in Linearfaktoren. Wegen $f \mid g$ gilt dasselbe für f. □

Erinnerung:
Der kleinste Teilkörper eines Körpers K wird der Primkörper von K genannt.

Satz (18.1)

Sei K ein Körper und P sein Primkörper.

(i) Ist $\mathrm{char}(K) = 0$, dann gilt $P \cong \mathbb{Q}$.

(ii) Ist $\mathrm{char}(K) = p$ für eine Primzahl p, dann gilt $P \cong \mathbb{F}_p$.

Die Elementezahl der endlichen Körper

Satz (18.2)

Ist K ein endlicher Körper, dann ist $|K|$ eine Primzahlpotenz. Es gilt also $|K| = p^n$ für eine Primzahl p und ein $n \in \mathbb{N}$.

Beweis von Satz 18.2

Sei K ein endlicher Körper z.zg.: Es gibt eine Primzahl p und ein $n \in \mathbb{N}$ mit $|K| = p^n$. Weil K ein Körper ist, ist $\text{char}(K)$ gleich 0 oder eine Primzahl. Im Fall $\text{char}(K) = 0$ wäre 1_K in $(K, +)$ ein Element unendl. Ordnung $\lightning$ da K endlich

also: $\text{char}(K) = p$ für eine Primzahl p

Sei P der Primkörper von K $\text{char}(K) = p \xRightarrow{\text{Prop. 18.1}}$

$P \cong \mathbb{F}_p$ Es ist $K | P$ eine Körpererweiterung und weil diese endl. ist, muss der Erw.-grad $n = [K : P]$ endlich sein.

$\Rightarrow K$ ist n-dim. P-Vektorraum $\Rightarrow |K| = |P|^n = |\mathbb{F}_p|^n = p^n$ $\square$

Formale Ableitung und mehrfache Nullstellen

Definition (18.3)

Sei K ein Körper und $f = \sum_{k=0}^{n} a_k x^k \in K[x]$, mit $n \in \mathbb{N}_0$ und $a_0, ..., a_n \in K$. Dann nennt man

$$f' = \sum_{k=1}^{n} k a_k x^{k-1}$$ die formale Ableitung von f.

Proposition (18.4)

Sei K ein Körper, $f \in K[x]$ ein Polynom vom Grad $n \geq 1$ und $\tilde{L}$ ein Erweiterungskörper von K, über dem f in Linearfaktoren zerfällt. Dann sind die folgenden beiden Aussage äquivalent:

(i) Es gilt $\mathrm{ggT}(f, f') = 1$ in $K[x]$.

(ii) Das Polynom f besitzt in $\tilde{L}$ nur einfache Nullstellen, d.h. es ein $a \in K^\times$ und n verschiedene Elemente $\alpha_1, ..., \alpha_n \in L$, so dass $f = a \prod_{i=1}^{n} (x - \alpha_i)$.

Beweis von Proposition 18.4

Var: $f \in K[x] \setminus K$ vom Grad n, $\tilde{L} \supseteq K$ Erweiterungskörper, über dem f in Linearfaktoren zerfällt

Zeige zunächst: Ist $\alpha \in \tilde{L}$ eine Nullstelle von f, dann gilt die Äquivalenz α ist mehrfache Nullst. von $f \iff f'(\alpha) = 0_K$

Da $f(\alpha) = 0_K$ gilt, existiert ein $g \in \tilde{L}[x]$ mit $f = (x - \alpha) \cdot g$.
Wie man leicht überprüft, gilt die Produktregel auch für formale Ableitungen. $\Rightarrow f' = g + (x - \alpha) g'$.

„$\Rightarrow$" α mehrfache Nullst. $\Rightarrow g(\alpha) = 0_K \Rightarrow f'(\alpha) = g(\alpha) + (\alpha - \alpha) \cdot g'(\alpha) = g(\alpha) + 0_K \cdot g'(\alpha) = 0_K$ „$\Leftarrow$" $f'(\alpha) = 0 \Rightarrow g(\alpha) + (\alpha - \alpha) \cdot g'(\alpha) = 0_K \Rightarrow g(\alpha) = 0_K \Rightarrow \alpha$ ist mehrf. Nullst. von f.

Wir beweisen nun die eigentl. Beh., d.h.

$ggT(f, f') = 1_K \iff f$ hat in $\tilde{L}$ nur einfache Nullstellen

„$\Longrightarrow$" Ang $ggT(f, f') = 1_K$ und α ist mehrfache Nullstelle von f. $\overset{\text{s.o.}}{\Longrightarrow} f'(\alpha) = 0_K$ Lemma von Bézout $\Rightarrow \exists u, v \in K[x]$ mit $uf + vf' = 1_K$

einsetzen $\Rightarrow 1_K = u(\alpha) f(\alpha) + v(\alpha) f'(\alpha) =$

$u(\alpha) \cdot 0_K + v(\alpha) \cdot 0_K = 0_K$ ↯ da K Körper

„$\Longleftarrow$" Vor.: f hat in $\tilde{L}$ nur einfache Nullst.

Ang. f, f' sind nicht teilerfremd. Dann existiert ein gem. Teiler $h \in K[x]$ vom Grad ≥ 1. Mit f zu-

$u(x) \cdot 0_K + v(x) \cdot 0_K = 0_K$ ↯ da K Körper

„⟸" Voraussetzung: $\tilde{L}$ nur einfache Nullst

fällt auch h in Linearfaktoren, insb. hat h in $\tilde{L}$ eine Nullstelle α. $h \mid f$, $h \mid f'$, $h(\alpha) = 0 \Rightarrow f(\alpha) = f'(\alpha) = 0_K \overset{\text{s.o.}}{\Rightarrow}$ α ist mehrfache Nullst. von f ↯. □

Endliche Körper als Zerfällungskörper

Proposition (18.5)

Sei p eine Primzahl, $n \in \mathbb{N}$ und K ein Körper mit p^n Elementen. Dann ist der Primkörper P von K zu $\mathbb{F}_p$ isomorph, und K ist ein Zerfällungskörper von $f_n = x^{p^n} - x \in P[x]$ über dem Körper P.

Beweis von Proposition 18.5

geg: Primzahl p, $n \in \mathbb{N}$, Körper K mit p^n Elementen

zzg: (i) $P \cong \mathbb{F}_p$ (ii) K ist Zerf.-körp. von $f = x^{p^n} - x \in P[x]$

zu (i) Sei $q = \mathrm{char}(K)$. Weil K endlich ist, ist q eine Primzahl. Weil q die Ordnung von 1_K in $(K, +)$ ist, gilt $q \mid p^n$. $\Rightarrow q = p$ $\overset{\text{Prop } 18.1}{\Rightarrow}$ $P \cong \mathbb{F}_p$

zu (ii) Beh.: Jedes $\alpha \in K$ ist Nullstelle von f.

1. Fall: $\alpha \in K$, d.h. $\alpha \in K^\times$ $\quad |K^\times| = p^n - 1$

$\Rightarrow \alpha^{p^n - 1} = 1_K \Rightarrow \alpha^{p^n} = \alpha \Rightarrow \alpha^{p^n} - \alpha = 0_K$

eine
$'(\alpha)$
□

$f(\alpha) = 0_K$. 2 Fall: $\alpha = 0_K$ Dann gilt

$f(\alpha) = f(0_K) = 0_K^{p^n} - 0_K = 0_K$ ($\Rightarrow$ Beh.)

Also besitzt f in K genau p^n Nullst. Wegen $\operatorname{grad}(f) = p^n$ folgt daraus, dass f über K in Linearfaktoren zerfällt. Da K durch die Menge K der Nullstellen über Prozent wird ($P(K) = K$), ist K insg. Zerfällungskörper von f über K. □