§ 17. Zerfällungskörper und normale Erweiterungen

Definition (17.1)

Sei $L|K$ eine Körpererweiterung und $f \in K[x]$ ein nicht-konstantes Polynom. Zerfällt f über L in Linearfaktoren, und bezeichnen $\alpha_1, ..., \alpha_r$ die Nullstellen von f in L, dann nennt man $K(\alpha_1, ..., \alpha_r)$ den Zerfällungskörper von f in L über dem Grundkörper K.

Satz (17.2)

Sei K ein Körper. Dann existiert zu jedem nicht-konstanten Polynom $f \in K[x]$ ein Zerfällungskörper von f über K.

Definition des algebraischen Abschlusses

Definition (17.6)

Ein Körper K heißt algebraisch abgeschlossen, wenn jedes nicht-konstante Polynom $f \in K[x]$ in K eine Nullstelle besitzt.

Definition (17.7)

Sei K ein Körper. Ein Erweiterungskörper L von K wird algebraischer Abschluss von K genannt, wenn $L|K$ algebraisch und L algebraisch abgeschlossen ist.

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

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 Prop. 17.17

geg.: normale Erweiterung $L|K$

M Zwischenkörper von $L|K$

Beh.: $M|L$ ist normal.

Sei $g \in L[x]$ ein (über L) irreduzibles Polynom

ist eine Nullstelle $\alpha \in L$. z.zg: g zerfällt über L

in Linearfaktoren

Sei $\tilde{g}$ die Normierung von g. klar: $\tilde{g} = \mu_{\alpha, M}$

Sei $f = \mu_{\alpha, K}$. Als Min.-pol. ist f irreduzibel in $K[x]$.

Sei $f = M_{\alpha,K}$. Als Min.-pol. ist f irreduzibel in $K[x]$

und f besitzt in L eine Nullstelle (nämlich α).

$L|K$ normal $\Rightarrow$ f zerfällt über L in Linearfaktoren

$f \in M[x]$, $\tilde{g} = M_{\alpha,M}$, $f(\alpha) = 0 \Rightarrow \tilde{g} \mid f$ in $M[x]$

$\Rightarrow g \mid f$ Mit f zerfällt somit auch g über L in Linear-

faktoren.

□

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 $P \cong \mathbb{F}_p$.

Beweis von Satz 18.1

geg: Körper K, mit Primkörper P

zu (i) Vor.: $\mathrm{char}(K) = 0$ z.zg.: $P \cong \mathbb{Q}$

Aus der Ringtheorie ist bekannt, dass ein eind. best. Ringhom. $\phi: \mathbb{Z} \to K$ existiert, geg. durch $\phi(n) = n \cdot 1_K$ $\forall n \in \mathbb{Z}$ (wobei $n \cdot 1_K$ die n-te additive Potenz von 1_K bezeichnet). Wegen $\mathrm{char}(K) = 0$ ist ϕ injektiv, denn: Ang. $\ker(\phi) \neq \{0\}$. $m \in \ker(\phi) \setminus \{0\}$ 1. Fall: $m \in \mathbb{N}$ $\to$

zu (2)

1_K

a.c

(1) $\Rightarrow$

$m \cdot 1_K = \phi(m) = 0$ ↯ zu $\operatorname{char}(K) = 0$

2. Fall: $-m \in \mathbb{N} \Rightarrow (-m) \cdot 1_K = \phi(-m) =$

$-\phi(m) = -0 = 0$ ↯ zu $\operatorname{char}(K) = 0$

Setze ϕ folgendermaßen zu einer Abb. $\hat{\phi}: \mathbb{Q} \to K$ fort: Ist $r \in \mathbb{Q}$ und sind $a \in \mathbb{Z}$, $b \in \mathbb{N}$ mit $r = \frac{a}{b}$ und $\operatorname{ggT}(a,b) = 1$ (Darstellung von r als gekürzter Bruch), dann definieren wir

$$\hat{\phi}(r) = \hat{\phi}\left(\frac{a}{b}\right) = \phi(a) \cdot \phi(b)^{-1}$$

(möglich, da K Körper und $\phi(b) \neq 0$)

Beh.: (1) Es gilt $\hat{\phi}\left(\frac{a}{b}\right) = \phi(a)\phi(b)^{-1}$ für alle $a \in \mathbb{Z}$ und $n \in \mathbb{N}$.

(2) Die Abbildung $\hat{\phi}$ ist ein Ringhom. (und damit ein Körperhomomorphismus, weil $\mathbb{Q}$ und K beides Körper sind).

zu (1) Seien $a \in \mathbb{Z}$, $b \in \mathbb{N}$, $r = \frac{a}{b} \in \mathbb{Q}$ und $r = \frac{a_1}{b_1}$ die Darstellung von r als gekürzter Bruch (d.h. $a_1 \in \mathbb{Z}$, $b_1 \in \mathbb{N}$, $ggT(a_1, b_1) = 1$). $\Rightarrow \frac{a}{b} = r = \frac{a_1}{b_1} \Rightarrow ab_1 = a_1 b$

$\Rightarrow \phi(a)\phi(b_1) = \phi(ab_1) = \phi(a_1 b) = \phi(a_1)\phi(b) \Rightarrow$

$\phi(a)\phi(b)^{-1} = \phi(a_1)\phi(b_1)^{-1} = \hat{\phi}\left(\frac{a_1}{b_1}\right) = \hat{\phi}(r) = \hat{\phi}\left(\frac{a}{b}\right)$

zu (2) Nach Def. gilt $\hat{\phi}(1) = \hat{\phi}\left(\frac{1}{1}\right) = \phi(1)\phi(1)^{-1} =$ (ϕ Ringhom)
$1_K \cdot 1_K^{-1} = 1_K$. Seien $r, s \in \mathbb{Q}$, $r = \frac{a}{b}$, $s = \frac{c}{d}$ mit
$a, c \in \mathbb{Z}$, $b, d \in \mathbb{N}$. $\Rightarrow r + s = \frac{ad + bc}{bd}$, $rs = \frac{ac}{bd}$

$\overset{(1)}{\Rightarrow} \hat{\phi}(r+s) = \phi(ad+bc)\phi(bd)^{-1} = \phi(ad)\phi(bd)^{-1} +$

$$\phi(bc)\phi(bd)^{-1} = \phi(a)\phi(d)\phi(b)^{-1}\phi(d)^{-1} +$$

$$\phi(b)\phi(c)\phi(b)^{-1}\phi(d)^{-1} = \phi(a)\phi(b)^{-1} + \phi(c)\phi(d)^{-1}$$

$$= \hat{\phi}\left(\frac{a}{b}\right) + \hat{\phi}\left(\frac{c}{d}\right) = \hat{\phi}(r) + \hat{\phi}(s), \text{ ebenso}$$

$$\hat{\phi}(rs) = \phi(ac)\phi(bd)^{-1} = \phi(a)\phi(c)\phi(b)^{-1}\phi(d)^{-1}$$

$$= \phi(a)\phi(b)^{-1}\phi(c)\phi(d)^{-1} = \hat{\phi}\left(\frac{a}{b}\right)\cdot\hat{\phi}\left(\frac{c}{d}\right) = \hat{\phi}(r)\,\hat{\phi}(s).$$

Da Körperhom. injektiv sind, definiert $\hat{\phi}$ ein Isom. zwischen $\mathbb{Q}$ und $\hat{\phi}(\mathbb{Q})$. Beh.: $\hat{\phi}(\mathbb{Q}) = P$

„$\supseteq$" Offenbar ist $\hat{\phi}(\mathbb{Q})$ ein Teilkörper von K. Da P nach Def. der kleinste Teilkörper ist, muss $P \subseteq \hat{\phi}(\mathbb{Q})$ gelten.

„$\subseteq$" P Teilkörper von $K \Rightarrow \phi(1) = 1_K \in P$

Vollst. Ind. über $m \in \mathbb{N} \Rightarrow \phi(m) \in P \; \forall m \in \mathbb{N}$. damit auch $\phi(-m) = -\phi(m) \in P \; \forall m \in \mathbb{N}$. insg. $\phi(\mathbb{Z}) \subseteq P$

Da P Teilkörper von K ist, gilt auch $\phi(a)\phi(b)^{-1} \in P$

$\forall a \in \mathbb{Z}, b \in \mathbb{N} \Rightarrow \hat{\phi}(\mathbb{Q}) \subseteq P$ ($\Rightarrow$ Beh.)

Also liefert $\hat{\phi}$ einen Isom. zwischen $\mathbb{Q}$ und P.

Beweis von Satz 18.1 (Forts.)

zu (ii) K Körper, P Primkörper von K

Vor. diesmal: $\mathrm{char}(K) = p$ (p Primzahl)

Beh.: $P \cong \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

Sei $\phi : \mathbb{Z} \to K$ der eind. best. Ringhom. von oben.

Beh: ϕ induziert einen Isom. $\mathbb{Z}/p\mathbb{Z} \cong P$ von Ringen (und damit von Körpern, da $\mathbb{Z}/p\mathbb{Z}$ und P beides Körper sind)

Nachweis mit Hilfe des Homomorphiesatzes für Ringe.

dafür zu überprüfen: (1) $\ker(\phi) = p\mathbb{Z}$

(2) $\operatorname{im}(\phi) = P$

zu (1) „$\supseteq$" $\operatorname{char}(K) = p \Rightarrow \phi(p) = p\,1_K = 0_K \Rightarrow p \in \ker(\phi)$

Da ϕ ein Gruppenhom. zwischen $(\mathbb{Z}, +)$ und $(K, +)$ ist, folgt $p\mathbb{Z} \subseteq \ker(\phi)$, da $p\mathbb{Z}$ mit der von p erzeugten Untergruppe $\langle p \rangle$ von $(\mathbb{Z}, +)$ übereinstimmt

„$=$" Ang. $\ker(\phi) \supsetneq p\mathbb{Z}$ Sei $m \in \ker(\phi) \setminus p\mathbb{Z} \overset{p \text{ Primz.}}{\Rightarrow} ggT(m, p) = 1$

Bézout $\Rightarrow \exists\, a, b \in \mathbb{Z}$ mit $1 = am + bp \underset{m, p \in \ker(\phi)}{\Rightarrow} 1 \in \ker(\phi)$

$\Rightarrow 0_K = \phi(1) = 1_K$ ↯ da K Körper

$\uparrow \phi$ Ringhom.

zu (2) „$\subseteq$" Wie in Teil (1) zeigt man $\phi(\mathbb{Z}) \subseteq P$

„$\supseteq$" Sei $\bar{\phi}$ der durch ϕ induzierte Ringhom. $\mathbb{Z}/p\mathbb{Z} \to K$. Dann ist $\operatorname{im}(\phi) = \phi(\mathbb{Z}) = \bar{\phi}(\mathbb{Z}/p\mathbb{Z})$ Da $\mathbb{Z}/p\mathbb{Z}$ Körper ist, ist

$\Phi(\mathbb{Z}/p\mathbb{Z})$ ein Teilkörper von K. Weil P der kleinste Teilkörp. von K ist, folgt damit

$P \subseteq \Phi(\mathbb{Z}/p\mathbb{Z}) = \phi(\mathbb{Z}) = \mathrm{im}(\phi)$.

Also liefert der Hom-satz tatsächlich einen Isom zwischen $\mathbb{F}_p$ und P. $\square$

Sei

Beh

„$\Rightarrow$

f in

Endl

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:

geg. endlicher Körper K

Sei P der Primkörper von K. Es gilt $\mathrm{char}(K) = p$ für eine Primzahl p, denn im Fall $\mathrm{char}(K) = 0$ wäre $P \cong \mathbb{Q}$ (*) $\Rightarrow$ P und K wären unendlich $\lightning$ zu $|K|$ endlich

(*) nach Satz 18.1

Nach Satz 18.1 gilt somit $P \cong \mathbb{F}_p \Rightarrow |P| = |\mathbb{F}_p| = p$. Nun ist $K | P$ eine endliche Erweiterung (da $|K|$ endlich). Sei $n = [K:P] \Rightarrow K$ ist n-dim. P-Vektorraum $\Rightarrow K \cong P^n$ (als P-Vektorraum)

$\Rightarrow |K| = |P|^n = p^n$ $\square$

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 Prop. 18.4:

geg: Körper K, $f \in K[x]$ vom Grad $n \geq 1$,
$\tilde{L} \supseteq K$ alg. abg Erweiterungskörper, z.Zg.:
Äquivalenz der Aussagen i) $\operatorname{ggT}(f, f') = 1$
ii) f hat in $\tilde{L}$ nur einfache Nullstellen

Sei zunächst $\alpha \in \tilde{L}$ eine bel. Nullstelle von f.

Beh.: α ist einfache Nullstelle von f $\iff$ $f'(\alpha) \neq 0_K$

„$\Rightarrow$": Ang. $f'(\alpha) = 0_K$. $f(\alpha) = 0_K \Rightarrow (x - \alpha)$ teilt f in $\tilde{L}[x] \Rightarrow \exists\, g \in \tilde{L}[x]$ mit $f = (x - \alpha) \cdot g$
Leicht zu überprüfen: Summen- und Produktregel gelten

auch für die formale Ableitung $\Rightarrow f' = g + (x-\alpha)\cdot g' \Rightarrow f'(\alpha) = g(\alpha) + (\alpha-\alpha)\cdot g'(\alpha) = g(\alpha) \Rightarrow g(\alpha) = f'(\alpha) = 0_K \Rightarrow (x-\alpha) \mid g$ in $\tilde{L}[x] \Rightarrow \exists h \in \tilde{L}[x] : g = (x-\alpha)\cdot h \Rightarrow f \overset{(\alpha)}{=} (x-\alpha)^2 \cdot h \Rightarrow \alpha$ mind. doppelte Nullst. von f

„$\Leftarrow$" Setze voraus, dass α mind. doppelte Nullstelle von f ist; also $(*)$ für ein $h \in \tilde{L}[x]$ gilt

$\Rightarrow f' = 2(x-\alpha)\cdot h + (x-\alpha)^2 \cdot h' \Rightarrow$

$f'(\alpha) = 2\cdot(\alpha-\alpha)\cdot h + (\alpha-\alpha)^2 \cdot h = 0_K$. ($\rightarrow$ Beh.)

Beweise nun die Äquivalenz.

„(i) $\Rightarrow$ (ii)": Ang. $ggT(f, f') = 1_K$ aber $\alpha \in \tilde{L}$ ist mehrfache Nullst. von f Beh $\Rightarrow f'(\alpha) = f(\alpha) = 0_K$

$ggT(f, f') = 1 \overset{\text{Bézout}}{\Rightarrow} \exists\, u, v \in K[x]$ mit $uf + vf' = 1_K$

$\Rightarrow 1_K = u(\alpha) f(\alpha) + v f'(\alpha) = u(\alpha) 0_K + v(\alpha) 0_K = 0_K$ ↯

„(ii) ⇒ (i)" Setze (ii) voraus, ang. f und f' sind nicht teilerfremd

$\Rightarrow \exists\, g \in K[x] \setminus K$, gem. Teiler von f und f'.

Da $\tilde{L}$ alg. abgeschlossen ist, besitzt g in $\tilde{L}$ eine Nullst. α.

$g \mid f$, $g \mid f' \Rightarrow \alpha$ ist gem. Nullst. von f und $f' \overset{\text{Beh}}{\Rightarrow}$

α ist mehrfache Nullst. von f ↯ zu (ii) □