Vorlesung Algebra

SoSe'21, hhu
K. Halupczok

Teil III: KÖRPER

A19: Zerfällungskörper

Stichworte: Erweiterungskörper zu verschiedenen Wurzeln eines Polynoms, Zerfällungskörper, ZK von T^p-1 und T^p-2, Fortsetzung eines Isomorphismus zwischen Körpern auf deren ZK, Zerfällung von irred. Polynomen über ZK in Linearfaktoren, normale Erweiterung

---

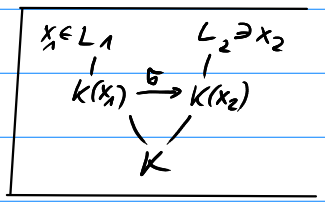
19.1. **Einleitung:** Körper können so erweitert werden, dass irreduzible Polynome Wurzeln in der Erweiterung bekommen. In einem Zerfällungskörper von f über K zerfällt f in Linearfaktoren.

19.2. **Satz:** Sei K Körper, $f \in K[T]$ irred. Dann:

(1) Es gibt einen Erw.körper $L|K$, in dem f eine Wurzel hat.

(2) Seien x_1, x_2 Wurzeln von f in $L_1|K$, $L_2|K$.

$\Rightarrow \exists!\ \sigma: K(x_1) \to K(x_2)$ Iso über K (d.h. $\sigma|_K = \mathrm{id}_K$) mit: $\sigma(x_1) = x_2$.



Bew.: (1): Sei $f = \sum_{i=0}^{n} a_i T^i \in K[T]$, und $L := K[T]/(f)$, ist Körper.

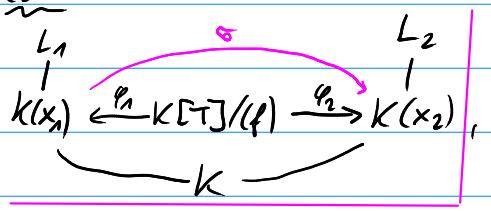
Ferner sei $\pi: K[T] \to L$ die Projektion nach (f).

Dann: $0 = \pi(f) = \sum_{i=0}^{n} (\pi a_i)(\pi T)^i$.

Somit: Identifiziere $a \in K$ mit $\pi(a) \in L$ ($\pi|_L$ ist ja injektiv), ferner setze $x = \pi T$.

Dann: $L|K$ und $0 = \sum_{i=0}^{n} a_i x^i = f(x)$.

(2): Situation:



, dabei φ_1, φ_2 Iso nach A18.17,

$\varphi_i: g + (f) \mapsto g(x_i)$.

Setze $\sigma := \varphi_2 \circ \varphi_1^{-1}$, dann: $\forall k \in K: \sigma(k) = \varphi_2 \circ \varphi_1^{-1}(k) = \varphi_2(k + (f)) = k$,

$\sigma(x_1) = \varphi_2 \circ \varphi_1^{-1}(x_1) = \varphi_2(T + (f)) = x_2$.

Eind.: Seien σ_1, σ_2 zwei solche Iso's, betr.

Körper $K_0 := \{y \in K(x_1);\ \sigma_1(y) = \sigma_2(y)\} \subseteq K(x_1)$.

Dann: $x_1 \in K_0$, $K \subseteq K_0 \Rightarrow K_0 \supseteq K(x_1)$. Somit: $K_0 = K(x_1)$, also $\sigma_1 = \sigma_2$. □

19.3. **Lemma:** Sei $\sigma: K \to K'$ Körperiso. Dann lässt sich σ eind. erw. zu Iso
$\bar{\sigma}: K[T] \to K'[T']$ mit $\bar{\sigma}(T) = T'$.

$$\begin{array}{ccc} K[T] & \xrightarrow{\bar{\sigma}} & K'[T'] \\ | & & | \\ K & \xrightarrow{\sigma} & K' \end{array}$$

Beweis: Univ. Eig. von Polynomringen:

$$\begin{array}{ccc} K & \xrightarrow{\sigma} & K' \subseteq K'[T'] \\ \downarrow & \nearrow & \\ K[T] & \exists!\, \bar{\sigma}\ \text{Iso},\ T \mapsto T' & \end{array}$$

$\bar{\sigma}: K[T] \to K'[T']$
$g = \sum_{i=0}^{n} a_i T^i \mapsto \sum_{i=0}^{n} (\sigma a_i) T'^i =: g^\sigma$.

□

19.4. **Def:** $g^\sigma := \sum_{i=0}^{n} (\sigma a_i) T'^i$ für $g = \sum_{i=0}^{n} a_i T^i \in K[T]$.

19.5. **Bem:** Für $g \in K[T]$, $x \in K$: $\sigma(g(x)) = g^\sigma(\sigma x)$

Insb.: $g(x) = 0 \Leftrightarrow g^\sigma(\sigma x) = 0$.

19.6. **Lemma:** Seien $L|K$, $L'|K'$ Körpererw., $f \in K[T]$ irred., $x \in L$ Wurzel von f.

$$\begin{array}{ccccc} L & & & & L' \\ | & & & & | \\ K(x) & & \xrightarrow{\bar{\sigma}} & & K'(x') \\ & \searrow & & \nearrow & \\ & & K \xrightarrow{\sigma} K' & & \\ & & f & & f^\sigma \end{array}$$

Ferner sei $\sigma: K \to K'$ ein Iso. Dann:

(1) $\forall$ Wurzel x' von f^σ $\exists!$ Forts. $\bar{\sigma}: K(x) \to K'(x')$ Iso von σ: $\bar{\sigma}(x) = x'$.

(2) $\#\{\bar{\sigma}: K(x) \to L' \text{ Einbett., Forts. von } \sigma\} = \#\{x' \in L';\ f^\sigma(x') = 0\}$.

Beweis: (1):

$$\begin{array}{ccc} K(x) & \xrightarrow{\bar{\sigma}} & K'(x') \\ \text{Iso} \uparrow \varphi_1 & & \text{Iso} \nearrow \varphi_2 \\ K[T]/(f) & \xrightarrow[\text{Iso (Hom.satz)}]{\Psi} & K'[T']/(f^\sigma) \\ \uparrow & & \uparrow \\ K[T] & \xrightarrow[\text{Iso, 19.3}]{\bar{\sigma}} & K'[T'] \\ & \searrow \quad \swarrow & \\ & K \xrightarrow[\text{Iso}]{\sigma} K' & \end{array}$$

Def. $\bar{\sigma} := \varphi_2 \circ \Psi \circ \varphi_1^{-1}$ Iso, Forts. von σ, mit

$\bar{\sigma}(x) = \varphi_2 \circ \Psi \circ \varphi_1^{-1}(x)$
$= \varphi_2 \circ \Psi(T + (f)) = \varphi_2(T' + (f^\sigma)) = x'$.

Eind., da $\varphi_2, \Psi, \varphi_1$ eind.

(2): $\#\text{l.S.} \geq \#\text{r.S.}$: Nach Teil (1) ✓

$\#\text{l.S.} \leq \#\text{r.S.}$: Sei $\bar{\sigma}: K(x) \to L'$ Einbettung, die σ fortsetzt.

Dann: $f^\sigma(\sigma x) = \sigma(f(x)) = \sigma(0) = 0$,

d.h. σx ist Wurzel von f^σ.

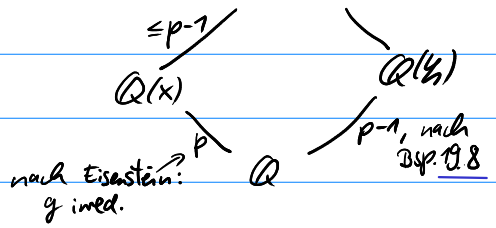
□

19.7. **Def.:** Sei $f \in K[T]$, $\deg(f) > 0$. $L|K$ Zerfällungskörper von f über K $:\Leftrightarrow$
$\exists x_1, \dots, x_m \in L \ \exists a \in K$: $\begin{cases} f(T) = a \prod_{i=1}^{m} (T - x_i), \\ L = K(x_1, \dots, x_m). \end{cases}$ Abk.: $L|K$ ist ZK von $f|K$.

19.8. **Bsp.:** Sei $p \in \mathbb{N}$ prim, $f = T^p - 1 \in \mathbb{Q}[T]$. Gesucht: ZK von $f|\mathbb{Q}$?
Es ist: $f(T) = (T-1)(T^{p-1} + \dots + T + 1) =: (T-1)\,\Phi_p(T)$.
Die Wurzeln von f in $\mathbb{C}$ sind die paarweise verschiedenen komplexen Zahlen
ζ^k, $0 \le k < p$, mit $\zeta := e^{2\pi i/p}$, die man p-te Einheitswurzeln nennt.
Somit: $f = \prod_{k=0}^{p-1} (T - \zeta^k) \in \mathbb{C}[T] \Rightarrow \Phi_p(T) = \prod_{\alpha=1}^{p-1} (T - \zeta^\alpha) \in \mathbb{C}[T]$

$\Rightarrow \mathbb{Q}(\zeta, \zeta^2, \dots, \zeta^{p-1}) = \mathbb{Q}(\zeta)$ ist ZK von $f|\mathbb{Q}$,
ferner: $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$.

19.9. **Bsp.:** Sei $p \in \mathbb{N}$ prim, $g(T) = T^p - 2 \in \mathbb{Q}[T]$. Gesucht: ZK von $g|\mathbb{Q}$?
Sei $x \in \mathbb{C}$ mit $x^p = 2$. Die Wurzeln von g sind also
$x, \zeta x, \zeta^2 x, \dots, \zeta^{p-1} x$, wobei $\zeta := e^{2\pi i/p}$.
Setze $L := \mathbb{Q}(x, \zeta x, \dots, \zeta^{p-1} x) = \mathbb{Q}(x, \zeta)$, ist ZK von $g|\mathbb{Q}$.
Ferner:



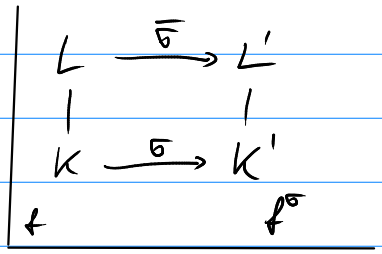
$\Rightarrow [L : \mathbb{Q}(x)] = [\mathbb{Q}(x, \zeta) : \mathbb{Q}(x)] \le [\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$,
da das Mipo von $\zeta|\mathbb{Q}$ auch Koeff. in $\mathbb{Q}(x)$ hat. Somit: $[L : \mathbb{Q}] \le p \cdot (p-1)$.
Da p und $p-1$ Teiler von $[L : \mathbb{Q}]$ sind, folgt: $[L : \mathbb{Q}] = p \cdot (p-1)$.

19.10. **Bsp:** Sei $L|K$ ZK eines $f \in K[T]$, $\deg(f) = m \Rightarrow [L : K] \le m!$.
Bew.: VI über m: $m = 1$: $L = K(x_1)$, $f(x_1) = 0 \Rightarrow [L : K] \le 1 = 1!$ ✓
$m \to m+1$: $f = g \cdot (T - x_{m+1}) \in K(x_{m+1})[T] \Rightarrow g \in K(x_{m+1})[T]$,
also $L = K(x_{m+1})(x_1, \dots, x_m)$ ZK von $g|K(x_{m+1})$, $\deg(g) = m$.
IV: $[L : K(x_{m+1})] = [K(x_{m+1})(x_1, \dots, x_m) : K(x_{m+1})] \le m!$
$\Rightarrow [L : K] = [L : K(x_{m+1})] \cdot [K(x_{m+1}) : K] \le m! \cdot [K(x_{m+1}) : K]$
$\le m! \,(m+1) = (m+1)!$ □

19.11. Satz: Sei K Körper, $f \in K[T]$, $\deg(f) = n > 0$. Dann:

(1) $\exists$ ZK von $f|K$,

(2) $\sigma: K \to K'$ Iso, $L|K$, $L'|K'$ ZK von $f|K$, $f^\sigma|K'$
$\Rightarrow \sigma$ fortsetzbar zu Iso $\bar\sigma: L \to L'$.



Bew.: (1): VI nach n: $n=1$: $f = aT - b \Rightarrow L := K(\frac{b}{a})$ ✓.

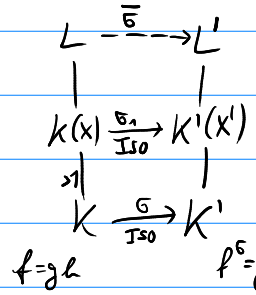
$n > 1$: Sei $f = f_1 g$, f_1 irred.

a) $\deg f_1 = 1$: IV $\rightsquigarrow$ ZK von $g|K$, sei dieser L', $f_1 = aT - b$
$\Rightarrow L := L'(\frac{b}{a}) = L'$ ist ZK von f.

b) $\deg f_1 > 1$: Satz 19.2 $\Rightarrow \exists K_1|K$ mit $f_1(x_1) = 0$, $x_1 \in K$.
Schreiben: $f_1 = (T - x_1) \cdot g_1$, $g_1 \in K_1[T]$.
IV auf $g_1 \cdot g | K_1 \Rightarrow L'$ ZK von $g_1 g | K_1$,
dann $L := L'(x_1)$ ZK von f.

(2): VI nach $n := [L:K]$: $n = 1$: $L = K$, $\bar\sigma = \sigma$. ✓

$n > 1$: Sei $f = g \cdot h$, $g \in K[T]$ irred. mit $\deg(g) > 1$, $g(x) = 0$.

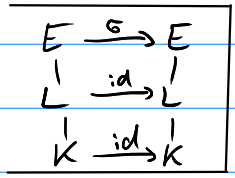


Nach 19.2.(2): Forts. $\sigma_1: K(x) \to K'(x')$,
wenn x' Wurzel von f^σ.

Nun ist: L ZK von $f|K(x)$,
L' ZK von $f^\sigma | K'(x')$,
ferner $[L : K(x)] < n$.

IV auf $\sigma_1: K(x) \to K(x')$, f, f^σ, L, L' liefert
eine Fortsetzung $\bar\sigma: L \to L'$ (Iso) von σ_1 bzw. σ. □

19.12. Satz: Sei $L|K$ endl. Dann sind äquivalent:



(1) L ist ZK eines $f \in K[T]$ über K.

(2) Für jeden Auto $\sigma: E \to E$, $E|L$, mit $\sigma|K = id_K$ gilt: $\sigma(L) = L$.

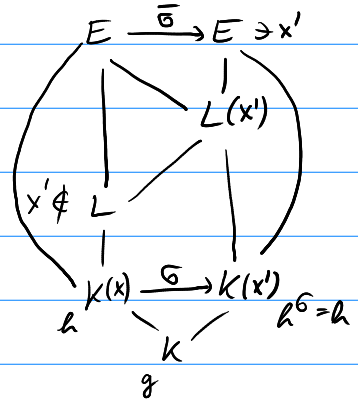
(3) Für jedes irred. $g \in K[T]$ mit: $(\exists x \in L: g(x) = 0)$ gilt:
g zerfällt über L in Linearfaktoren.

Bew.: (1)⇒(2): Sei $L = K(x_1, \dots, x_m)$, $x_1, \dots, x_m$ die Wurzeln von $f \in K[T]$,
sei $f = \sum_{i=0}^{m} a_i T^i$ und $\sigma : E \to E$ Auto, E/L, $\sigma|_K = id_K$.

Dann: $0 = \sigma(f(x_j)) = \sum_{i=0}^{m} (\sigma a_i)(\sigma x_j)^i = f(\sigma x_j)$.
($\sigma a_i = a_i$)

Also: $\{\sigma x_1, \dots, \sigma x_m\} = \{x_1, \dots, x_m\} \Rightarrow \sigma L = \sigma K(x_1, \dots, x_m) = K(x_1, \dots, x_m) = L$.

(2)⇒(3): Sei $L = K(x_1, \dots, x_m)$, $g_i \in K[T]$ seien die Mipo von x_i, $1 \le i \le m$.



Sei $g \in K[T]$ irred. mit Wurzel $x \in L$,
sei E/L ein Zk von $g \cdot g_2 \cdot \dots \cdot g_m =: h$ über K.
Ann.: $\exists$ Wurzel $x' \in E$ von g, $x' \notin L$.
Nach Lemma 19.6 ex. Iso $\sigma : K(x) \to K(x')$, $\sigma|_K = id_K$.
E ist Zk von $h/K(x)$,
E ist Zk von $h^\sigma = h/K(x')$.
Nach Satz 19.11 ex. forts. $\bar{\sigma} : E \to E$,
Auto mit $\bar{\sigma}(x) = x' \notin L \overset{(2)}{\Rightarrow} x \notin L$ ↯.

(3)⇒(1): Sei $L = K(x_1, \dots, x_m)$, und $g_i \in K[T]$ seien die Mipo von x_i/K, $1 \le i \le m$,
sei $g := g_1 \cdot \dots \cdot g_m$. Da die g_i in L in Linearfaktoren zerfallen,
ist also L ein Zk von g/K. □

19.13. **Def.:** Eine endl. Erw. L/K heißt **normal**, wenn eine der Bed. (1), (2) oder (3)
aus Satz 19.12 erfüllt ist.