

Vorlesung Algebra

SoSe'21, hhu

Teil IV: und zurück (GALOISTHEORIE)

K. Halupczok

A24: Radikal erweiterungen

Stichworte: Radikal erweiterung, Radikalturm, Auflösbar durch Radikale, lineare Unabhängigkeit von Charakteren, (reine) Wurzeln und zyklische Galois erweiterungen, normale Hülle, normale Hülle separabler Radikal erweiterungen

24.1. Einleitung: Die Frage, ob die Nullstellen eines separablen Polynoms stets durch eine Lösungsformel (wie die p-q-Formel für quadratische Polynome) berechenbar ist, führt zum Begriff der Auflösbarkeit durch Radikale und kann im Rahmen der Körpertheorie durch Radikal erweiterungen beschrieben werden, wobei zyklische Galois erweiterungen eine wesentliche Rolle spielen. Der Übergang zur normalen Hülle von Radikal erweiterungen sorgt dafür, dass die Galoistheorie greifen kann.

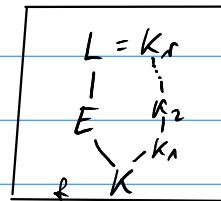
24.2. Def: Körperew. L/K heißt Radikal erweiterung : $\Leftrightarrow \exists$  Körperum

$$\textcircled{*} \quad K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_r = L;$$

H0  $\forall i < r: K_{i+1} = K_i(x_i)$  für ein  $x_i \in K_{i+1}$  mit  $x_i^m \in K_i$  für ein  $m \in \mathbb{N}$ .

\* heißt ein Radikalturm für L/K vom Typ  $(m_0, m_1, \dots, m_{r-1})$ .

24.3. Bem.:  $K_{i+1}$  entsteht aus  $K_i$  durch Adjunktion einer Wurzel eines „reinen“ Polynoms der Form  $T^{m_i} - a \in K_i[T]$ .



24.4. Def.: Ein sep.  $f \in K[T]$  heißt auflösbar durch Radikale : $\Leftrightarrow$

$\exists$  Radikal ew. von  $L/K$ , die einen ZK von  $f$  über  $K$  enthält.

Wir zeigen den Hilfssatz 24.5, der auch schon im Rahmen der Gruppentheorie behandelt werden kann. Es geht dabei um (Gruppen-)charaktere. Einen Gruppenhomomorphismus von einer Gruppe  $G$  in die multiplikative Gruppe  $K^\times$  eines Körpers  $K$  nennt man Charakter. Der Fall  $G = (\mathbb{Z}/m\mathbb{Z})^\times$  und  $K = \mathbb{C}$  ist besonders für die Zahlentheorie von Interesse.

## 24.5. Satz (Lineare Unabhängigkeit von Charakteren):

Sei  $G$  Gruppe,  $K$  Körper,  $\chi_1, \dots, \chi_m : G \rightarrow K^\times$  pwv. Gruppenhom.

Dann:  $\chi_1, \dots, \chi_m$  lin. unabh. im  $K$ -VR aller FKtn.  $G \rightarrow K$ .

Bew.: Sonst:  $\chi_1, \dots, \chi_m$  Gegenbsp. mit  $m$  minimal, also

$$a_1 \chi_1 + \dots + a_m \chi_m = 0 \text{ für gewisse } a_i \in K, \text{ nicht alle } a_i = 0.$$

Somit: Alle  $a_i \neq 0$ ,  $m > 1$ .

$$\forall g \in G: \sum_{i=1}^m a_i \chi_i(g) = 0, \text{ und da } \chi_1 \neq \chi_2,$$

$$\text{ex. } h \in G: \chi_1(h) \neq \chi_2(h).$$

$$\text{Dann: } \sum_{i=1}^m a_i \chi_i(h) \chi_i(g) = \sum_{i=1}^m a_i \chi_i(hg) = 0 \quad \forall g \in G.$$

$$\text{Weiter ist: } \sum_{i=1}^m a_i \chi_1(h) \chi_i(g) = 0 \quad \forall g \in G.$$

$$\text{Somit: } \forall g \in G: \sum_{i=2}^m a_i \underbrace{(\chi_i(h) - \chi_1(h))}_{\neq 0 \text{ für } i=2} \chi_i(g) = 0,$$

im  $\downarrow$  zur minimalen Wahl von  $m$ .  $\square$

24.6. Kor.: Sei  $L/K$  galois,  $\sigma_1, \dots, \sigma_m \in \text{Gal}(L/K)$  pwv. Dann:

$\sigma_1, \dots, \sigma_m$   $L$ -lin. unabh. im  $L$ -VR aller FKtn.  $L \rightarrow L$ .

Bew.: Anwenden von Satz 24.5 auf  $\sigma_1|L^\times, \dots, \sigma_m|L^\times : L^\times \rightarrow L^\times$

liefert die  $L$ -lineare Unabhängigkeit von  $\sigma_1, \dots, \sigma_m$ .  $\square$

24.7. Satz:  $K$  enthalte die  $m$ -ten Einheiten, d.h.  $T^m - 1$  zerfällt  $| K$ , char  $K$  fm.

Dann gilt: (1)  $x$  Wurzel (in  $L/K$ ) eines  $T^m - a$  ( $a \in K$ )

$\Rightarrow K(x)|K$  zyklische Galoiserw.,  $[K(x):K] | m$ .

(2)  $\forall$  zykl. Erw.  $L/K$ ,  $[L:K] = m$ ,  $\exists x \in L$ :

$L = K(x)$  und  $x^m \in K$ .

Bew.: (1): Sei  $E_m$  die zyklische Gruppe der  $m$ -ten Einheiten.

$\Rightarrow$  Wurzeln von  $T^m - a$  in  $L$  sind die El.  $\xi_x, \xi \in E_m$ .

Sei  $G = \text{Gal}(K(x)/K)$ .

$$\exists \sigma \in G \quad \exists \xi_\sigma \in E_m: \sigma x = \xi_\sigma x.$$

Nun:  $G \rightarrow E_m$ ,  $\sigma \mapsto \xi_\sigma$ , ist inj. Gruppenhom.

$$\begin{aligned} \text{Für inj.: } \sigma &\mapsto \xi_\sigma \\ \Rightarrow \sigma x &= x, \sigma = \text{id} \end{aligned}$$

Gruppenhom.:  $\xi_{\sigma\tau} x = \sigma(\tau(x)) = \sigma(\xi_\tau x) = \xi_\sigma \xi_\tau x$ . Somit:  $G$  zyklisch,  $\#G | m$ .

(2): Sei  $\text{Gal}(L/K) = \langle \sigma \rangle$ , schreiben:  $T^m - 1 = f(T) \cdot (T - \zeta)$ ,

wobei  $\zeta \in K$  primitive  $m$ -te EW,  $f \in K[T]$

Betr. Ringhom.  $K[T] \rightarrow K[\sigma]$ .

$\left[ \begin{array}{l} \in \text{End}_K(L), \text{ der } K\text{-Algebra} \\ \text{der } K\text{-VR-Endos des } K\text{-VRs } L \end{array} \right]$

$$\sigma^m = e \Rightarrow 0 = \underbrace{\zeta^m - 1}_{\zeta^{m-1} + a_{m-2} \zeta^{m-2} + \dots + a_1 \zeta + a_0} = f(\zeta)(\zeta - 1)$$

$$\zeta^{m-1} + a_{m-2} \zeta^{m-2} + \dots + a_1 \zeta + a_0$$

Da  $\deg f \leq m-1$ , ist  $f(\zeta) \neq 0$  nach Kor. 24.6.

$\Rightarrow \zeta - 1$  nicht surjektiv, also insb. nicht injektiv.

\* Sei  $x \in L^*$  ein Eigenvektor von  $\sigma$  zum Eigenwert  $\zeta$ , d.h.  $\sigma x = \zeta x$ .

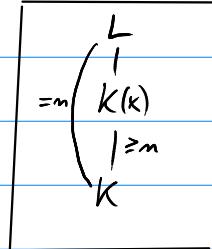
$$\Rightarrow \sigma^i x = \zeta^i x, 0 \leq i \leq m.$$

$\Rightarrow$  Die  $m$  Einbettungen  $\sigma^i|_{K(x)}: K(x) \rightarrow L$  sind pwv.

$\Rightarrow [K(x):K] \geq m$  nach Lemma A20.11.

Somit:  $K(x) = L$ .

Wegen  $\sigma(x^m) = (\sigma x)^m = (\zeta x)^m = \zeta^m x^m = x^m$  ist  $x^m \in \text{Fix}(\sigma) = K$ .  $\square$



24.8. Lemma: Sei  $L/K$  sep. und endl. Dann  $\exists! E \subset L$  mit:

$\boxed{\begin{array}{l} E \rightarrow F \\ \text{norm.} \\ \& \text{sep.} \\ \hline L \\ \text{sep.} \\ \hline K \end{array}}$  (1)  $E \subset K$  norm. und separabel.  
 (2)  $\forall F \subset L$  mit  $F \subset K$  norm.  
 $\exists \sigma: E \rightarrow F$  inj. über  $L$ .

Bew.: Satz vom primitiven El. A20.16  $\Rightarrow \exists \alpha \in L: L = K(\alpha)$ .

Sei  $f$  das Mipo von  $\alpha$  über  $K$ ,

$E := \mathbb{Z}K$  von  $f|_K$ .

Dann:  $E \subset K$  norm. und separabel, da  $L = K(\alpha)$  sep.  $|K$

$\xrightarrow{\text{A20.12}} \alpha$  sep., d.h. (1)

und:  $F \subset K$  norm.,  $F \subset L \Rightarrow F \supseteq E$ , d.h. (2).

Somit ist  $E$  auch eind. bestimmt.  $\square$

24.9. Def.:  $E$  aus 24.8 heißt normale Hülle von  $L/K$ .

24.10. Lemma: Die normale Hülle  $E$  einer sep. Radikal erw.  $L/K$   
ist eine sep. Radikal erw.  $E/L/K$ .

Bew.: Sei  $K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_r = L$  ein Radikal turm für  $L/K$ .

Sei  $\text{Gal}(E/L) = \{\text{id} = \delta_1, \dots, \delta_m\}$ ,  $K_{i+n} = K_i(x_i)$ .

$\Rightarrow K = K_0 \subseteq K(x_0) \subseteq K(x_0, x_1) \subseteq \dots \subseteq K(x_0, \dots, x_{r-1}) = L$ .

Für  $1 \leq j \leq m$ :  $K = K_0 \subseteq K(\delta_j x_0) \subseteq K(\delta_j x_0, \delta_j x_1) \subseteq \dots \subseteq K(\delta_j x_0, \dots, \delta_j x_{r-1})$   
ist Radikal turm, und

$$E = K(\underbrace{\delta_1 x_0, \dots, \delta_1 x_{r-1}}_{=\text{id}}, \underbrace{\delta_2 x_0, \dots, \delta_2 x_{r-1}}, \dots, \underbrace{\delta_m x_0, \dots, \delta_m x_{r-1}})$$

ferner gilt:

$$K \subseteq K(x_0) \subseteq K(x_0, x_1) \subseteq \dots \subseteq K(x_0, \dots, x_{r-1}) =: K_r = L$$

$$\subseteq K_1(\delta_2 x_0) \subseteq K_1(\delta_2 x_0, \delta_2 x_1) \subseteq \dots \subseteq K_1(\delta_2 x_0, \dots, \delta_2 x_{r-1}) =: K_2$$

$\subseteq \dots$

$$\subseteq K_{m-1}(\delta_m x_0) \subseteq K_{m-1}(\delta_m x_0, \delta_m x_1) \subseteq \dots \subseteq K_{m-1}(\delta_m x_0, \dots, \delta_m x_{r-1}) = E$$

ist Radikal turm für  $E/L/K$ . □