# Vorlesung Algebra

SoSe'21, hhu
K. Halupczok

## Teil IV: und zurück (GALOISTHEORIE)

### A24: Radikalerweiterungen

Stichworte: Radikalerweiterung, Radikalturm, auflösbar durch Radikale, lineare Unabhängigkeit von Charakteren, (reine) Wurzeln und zyklische Galoiserweiterungen, normale Hülle, normale Hülle separabler Radikalerweiterungen

---

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 Radikalerweiterungen beschrieben werden, wobei zyklische Galoiserweiterungen eine wesentliche Rolle spielen. Der Übergang zur normalen Hülle von Radikalerweiterungen sorgt dafür, dass die Galoistheorie greifen kann.

24.2. Def.: Körpererw. $L|K$ heißt Radikalerweiterung $:\Leftrightarrow$ $\exists$ Körperturm

$$(*)\quad K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_r = L:$$

$\forall\, 0 \le i < r$: $K_{i+1} = K_i(x_i)$ für ein $x_i \in K_{i+1}$ mit $x_i^{m_i} \in K_i$ für ein $m_i \in \mathbb{N}$.

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

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 $:\Leftrightarrow$ $\exists$ Radikalerw. von $L|K$, die einen ZK von $f$ über $K$ enthält.

$$\begin{tikzcd}
L = K_r \arrow[d, dash] & \\
E \arrow[d, dash] & K_2 \arrow[u, dotted, dash] \arrow[d, dash] \\
K \arrow[ur, dash] & K_1 \arrow[u, dash]
\end{tikzcd}$$

$f$

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, $\chi_1, \dots, \chi_n : G \to K^\times$ pww. Gruppenhom.

Dann: $\chi_1, \dots, \chi_n$ lin. unabh. im $K$-VR aller Fktn. $G \to K$.

Bew.: Sonst: $\chi_1, \dots, \chi_n$ Gegenbsp. mit $n$ minimal, also

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

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

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

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

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

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

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

im ↯ zur minimalen Wahl von $n$. □

24.6 **Kor.:** Sei $L|K$ galois, $\sigma_1, \dots, \sigma_n \in \mathrm{Gal}(L|K)$ pww. Dann:

$\sigma_1, \dots, \sigma_n$ $L$-lin. unabh. im $L$-VR aller Fktn. $L \to L$.

Bew.: Anwenden von Satz 24.5 auf $\sigma_1 \restriction L^\times, \dots, \sigma_n \restriction L^\times : L^\times \to L^\times$

liefert die $L$-lineare Unabhängigkeit von $\sigma_1, \dots, \sigma_n$. □

24.7 **Satz:** $K$ enthalte die $n$-ten EWeln, d.h. $T^n - 1$ zerfällt $|K$, $\mathrm{char}\, K \nmid n$.

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

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

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

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

Bew.: (1): Sei $E_n$ die zyklische Gruppe der $n$-ten EWeln.

$\Rightarrow$ Wurzeln von $T^n - a$ in $L$ sind die El. $\zeta x$, $\zeta \in E_n$.

Sei $G = \mathrm{Gal}(K(x)|K)$.

Zu $\sigma \in G$ $\exists\, \zeta_\sigma \in E_n$: $\sigma x = \zeta_\sigma x$.

Nun: $G \to E_n$, $\sigma \mapsto \zeta_\sigma$, ist inj. Gruppenhom. ⌈inj.: $\sigma \mapsto 1 \Rightarrow \sigma x = x, \sigma = id$⌋

⌈Gruppenhom.: $\zeta_{\sigma\tau} x = \sigma\tau(x) = \sigma(\zeta_\tau x) = \zeta_\sigma \zeta_\tau x$.⌋ Somit: $G$ zyklisch, $\#G \mid n$.

(2): Sei $\mathrm{Gal}(L|K) = \langle \sigma \rangle$, schreiben: $T^n - 1 = f(T)\cdot(T-\zeta)$,
wobei $\zeta \in K$ primitive $n$-te EW, $f \in K[T]$.
Betr. Ringhom. $K[T] \to K[\sigma]$. $\left[\in \mathrm{End}_K(L)\text{, der } K\text{-Algebra der } K\text{-VR-Endos des } K\text{-VRs } L\right]$

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

Da $\deg f \leq n-1$, ist $f(\sigma) \neq 0$ nach Kor. 24.6.
$\Rightarrow \sigma - \zeta$ nicht surjektiv, also insb. nicht injektiv.
* Sei $x \in L^\times$ ein Eigenvektor von $\sigma$ zum Eigenwert $\zeta$, d.h. $\sigma x = \zeta x$.
$\Rightarrow \sigma^i x = \zeta^i x$, $0 \leq i \leq n$.
$\Rightarrow$ Die $n$ Einbettungen $\sigma^i \restriction K(x): K(x) \to L$ sind pwv.
$\Rightarrow [K(x):K] \geq n$ nach Lemma A20.11.
Somit: $K(x) = L$.

$$\begin{tikzcd} L \arrow[d, dash] \\ K(x) \arrow[d, dash, "\geq n"] \\ K \end{tikzcd} \quad = n$$

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

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

$$\begin{tikzcd} E \arrow[r] & F \\ L \arrow[u, dash] \arrow[ur, dash] & \\ K \arrow[u, dash, "\text{sep.}"] & \end{tikzcd} \quad \text{norm. \& sep.}$$

(1) $E|K$ normal und separabel.
(2) $\forall\, F|L$ mit $F|K$ normal
$\exists\, \sigma: E \to F$ 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 $K$,
$E := ZK$ von $f|K$.
Dann: $E|K$ normal und separabel, da $L = K(\alpha)$ sep. $|K$
$\overset{\text{A20.12}}{\Rightarrow}$ $\alpha$ sep., d.h. (1)
und: $F|K$ normal, $F|L \Rightarrow F \supseteq E$, 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. Radikalerw. $L|K$ ist eine sep. Radikalerw. $E|K$.

**Bew.:** Sei $K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_r = L$ ein Radikalturm für $L|K$.

Sei $\mathrm{Gal}(E|K) = \{id = \sigma_1, \ldots, \sigma_m\}$, $K_{i+1} = K_i(x_i)$.

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

Für $1 \leq j \leq m$: $K = K_0 \subseteq K(\sigma_j x_0) \subseteq K(\sigma_j x_0, \sigma_j x_1) \subseteq \ldots \subseteq K(\sigma_j x_0, \ldots, \sigma_j x_{r-1})$ ist Radikalturm, und

$$E = K(\underbrace{\sigma_1}_{=id} x_0, \ldots, \sigma_1 x_{r-1}, \sigma_2 x_0, \ldots, \sigma_2 x_{r-1}, \ldots, \sigma_m x_0, \ldots, \sigma_m x_{r-1}).$$

Ferner gilt:

$$\begin{aligned}
K &\subseteq K(x_0) \subseteq K(x_0, x_1) \subseteq \ldots \subseteq K(x_0, \ldots, x_{r-1}) =: K_1 = L \\
&\subseteq K_1(\sigma_2 x_0) \subseteq K_1(\sigma_2 x_0, \sigma_2 x_1) \subseteq \ldots \subseteq K_1(\sigma_2 x_0, \ldots, \sigma_2 x_{r-1}) =: K_2 \\
&\subseteq \ldots\ldots \\
&\subseteq K_{m-1}(\sigma_m x_0) \subseteq K_{m-1}(\sigma_m x_0, \sigma_m x_1) \subseteq \ldots \subseteq K_{m-1}(\sigma_m x_0, \ldots, \sigma_m x_{r-1}) = E
\end{aligned}$$

ist Radikalturm für $E|K$. $\square$