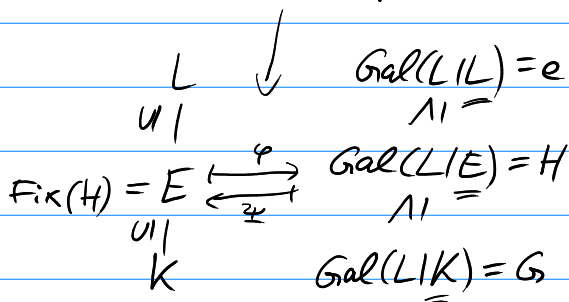


Galois-Korrespondenz

HS der Galoistheorie:



$$1. \left\{ \begin{array}{l} \text{Gal}(L|\text{Fix}(H)) = H \\ \text{Fix}(\text{Gal}(L|E)) = E \end{array} \right\}$$

$$2. \text{Gal}(E|K) \cong G/H$$

$$\text{Gal} \Rightarrow G = H \oplus G/H \cong \underbrace{\text{Gal}(L|E)}_{\cong H} \oplus \underbrace{\text{Gal}(E|K)}_{\cong G/H}$$

A24: Radikalerweiterungen

24.1. Einleitung: Polynome auflösbar durch Radikale $\iff$ Radikalerweiterungen

24.2. Def.: Eine Körpererweiterung $L|K$ heißt Radikalerweiterung : $(=)$

$$\exists \text{ Körperturm } K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \dots \subseteq K_r = L : \quad (*)$$

$$\forall 0 \leq i < r : K_{i+1} = K_i(x_i) \text{ für ein } x_i \in K_{i+1}$$

$$\text{mit } x_i^{m_i} \in K_i \text{ für ein } m_i \in \mathbb{N}.$$

$(*)$ heißt ein Radikalturm für $L|K$

von Typ $(m_0, m_1, \dots, m_{r-1})$.

Falls alle $m_i \leq 2$, heißt der zugehörige Radikalturm ein Quadratwurzelturm (QWT).

Bsp.: $\mathbb{Q}(\sqrt{2}, \sqrt[3]{4}) = K_r = L$

$$\begin{array}{c}
 \mathbb{Q}(\sqrt{2}, \sqrt[3]{4}) = K_r = L \\
 \uparrow \text{31} \\
 \mathbb{Q}(\sqrt{2}) = K_1 \\
 \uparrow \text{21} \\
 \mathbb{Q} = K_0
 \end{array}
 \begin{array}{l}
 \nearrow x_1 = \sqrt[3]{4} \rightarrow x_1^3 = 4 \rightarrow m_1 = 3 \\
 \nearrow x_0 = \sqrt{2} \rightarrow x_0^2 = 2 \rightarrow m_0 = 2
 \end{array}$$

ist Radikalturm, kein QWT

$$\begin{array}{c}
 \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}) \\
 \uparrow \\
 \mathbb{Q}(\sqrt{2}) \\
 \uparrow \\
 \mathbb{Q}
 \end{array}$$

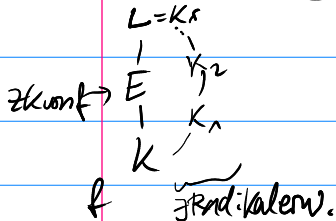
Haben: $L = K_r$

$$\begin{array}{c}
 K_r \\
 \vdots \\
 K_{i+1} = K_i(x_i), \quad x_i^{m_i} \in K_i \\
 \vdots \\
 K_1 = K_0 = K
 \end{array}$$

" $m_i \sqrt[n]{a}$ "

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 separables Polynom $f \in K[T]$ heißt auflösbar durch Radikale $\Leftrightarrow \exists$ Radikalerw. von $L|K$, die einen $\mathbb{Z}K$ von f über K enthält.



Bem.: Alle Wurzeln/Nst. von f können durch sukzessive Wurzelbildung (in L) ausgedrückt werden.

Bsp.: $f = T^{10} - 4T^5 + 1 \in \mathbb{Q}[T]$

$$= T^{10} - 4T^5 + 4 - 3$$

$$= (T^5 - 2)^2 - 3 \rightarrow (T^5 - 2)^2 = 3 \rightarrow T^5 - 2 = \pm \sqrt{3}$$

"ist auflösbar durch Radikale"

$$\mathbb{Q}(\sqrt{3}, \sqrt[5]{2+\sqrt{3}}, \zeta) = L$$

$$\mathbb{Q}(\sqrt{3}, \sqrt[5]{2+\sqrt{3}})$$

$$\mathbb{Q}(\sqrt{3})$$

$$\mathbb{Q} = K$$

$$\begin{aligned} & \mathbb{Q}(\zeta, \sqrt{3}, \sqrt[5]{2+\sqrt{3}}) \\ & \downarrow \\ & \mathbb{Q}(\zeta, \sqrt{3}) \\ & \downarrow \\ & \mathbb{Q}(\zeta) \end{aligned}$$

$$\rightarrow T^5 = 2 \pm \sqrt{3}$$

$$\xrightarrow{\sqrt[5]{}} T = \sqrt[5]{2 \pm \sqrt{3}}$$

Alle Wurzeln: $T = (e^{\frac{2\pi i j}{5}})^{\frac{1}{5}} \cdot \sqrt[5]{2 \pm \sqrt{3}}$
 $j = 0, \dots, 4$

$\mathbb{Z}K$ ist $\mathbb{Q}(\sqrt{3}, \sqrt[5]{2+\sqrt{3}}, \zeta)$, $\zeta := e^{2\pi i/5}$

Zunächst: Hilfsmittel der Gruppentheorie:

24.5. Satz (Lineare Unabhängigkeit von Charakteren):

Sei G Gruppe, K Körper, $\chi_1, \dots, \chi_m: G \rightarrow K^\times = K \setminus \{0\}$ p.w.v. Gruppenhom. (d.h. Charaktere). Dann: $\chi_1, \dots, \chi_n$ lin. unabh. im K -VR aller Fktn. $G \rightarrow K$.

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

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

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

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

- 3 -

$$\text{Dann: } \sum_{i=1}^m a_i \underbrace{\chi_i(h)}_{\chi_i \text{ Char.}} \underbrace{\chi_i(g)}_{\chi_i \text{ Char.}} = \sum_{i=1}^m a_i \chi_i(hg) = 0$$

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

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

↪ zur Min. von m . $\square$

24.6. Kor.: Sei $L|K$ galois, $\sigma_1, \dots, \sigma_m \in \text{Gal}(L|K)$ p.w.v. Dann:

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

Bew.: Anwenden von 24.5 auf $\sigma_1 \upharpoonright L^\times, \dots, \sigma_m \upharpoonright L^\times : L^\times \rightarrow L^\times$
liefert die L -lin. Unabh. von $\sigma_1, \dots, \sigma_m$. $\square$

24.4 Satz: K enthalte die n -ten EWeln, d.h. $T^n - 1$ zerfällt in K , $\text{char } K \nmid n$.

Dann: (1) x Wurzel (in $L|K$) eines $T^n - a$ ($a \in K$)
 $\Rightarrow K(x)|K$ zyklische Galois-erw., $[K(x):K] \mid n$.

(2) $\nexists$ zykl. ^{Galois-}Erw. $L|K$, $[L:K] = n$, $\exists x \in L$:
 $\uparrow$ $L = K(x)$ und $x^n \in K$.

^{$L|K$} Erinnerung: zyklische Galois-erw.
 $\Leftrightarrow \text{Gal}(L|K)$ zykl. Gruppe

Bew.:

(1): Sei E_n die zykl. Gr. der n -ten EWeln.

Als UG der mult. Gr. eines Körpers ...

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

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

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

ist inj. Gruppenhom. Gr.hom.: $\zeta_{\sigma\tau} x = \sigma\tau(x) = \sigma(\zeta_\tau x) = \zeta_\sigma \zeta_\tau x$.

inj.: $\sigma \mapsto 1 \Rightarrow \sigma x = x, \sigma = \text{id}$

Somit: G zyklisch, $\#G \mid n$.
 $= [K(x):K]$

$$\{\underbrace{\sigma^0, \sigma^1, \dots, \sigma^{m-1}}_{e=id_K}, \underbrace{\sigma^m = \sigma^0 = e}_{\downarrow}\}$$

(2): Sei $\text{Gal}(L|K) = \langle \sigma \rangle$, schreiben: $T^m - 1 = \underbrace{f(T) \cdot (T - \xi)}$,
wobei $\xi \in K$ primitive m -te EW, $f \in K[T]$.
(da alle m -ten EW enthält)

Betr. Ringhom. $K[T] \rightarrow K[\sigma]$. $\sigma \in \text{End}_K(L)$, die K -Algebra
 $T \mapsto \sigma$ der VR-Endos des K -VR L

$$\sigma^m = e \Rightarrow 0 = \sigma^m - e = \underbrace{f(\sigma)}_{\substack{\uparrow \\ \sigma\text{-Endo}}} (\underbrace{\sigma - \xi}_{\neq 0}) = \underbrace{f(\sigma) \circ (\sigma - \xi)}_{\neq 0}$$

$$f(\sigma) = \sigma^{m-1} + a_{m-2} \sigma^{m-2} + \dots + a_1 \sigma + a_0.$$

Da $\deg f \leq m-1$, ist $f(\sigma) \neq 0$ nach Kor. 24.6 (=lin. Unabh. der σ^i).

$\Rightarrow \sigma - \xi$ ist nicht surj. (sonst wäre $f(\sigma)$ die Nullabb.)

$\Rightarrow \sigma - \xi$ ist nicht inj.

$\Rightarrow$ also ex. $x \neq 0$ mit $(\sigma - \xi)x = 0 \Leftrightarrow \underline{\sigma x = \xi x}$.

* Sei $x \in L^\times$ ein Eigenvektor von σ zum Eigenwert ξ , d.h. $\sigma x = \xi x$.

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

$\Rightarrow$ Die m Einbettungen $\sigma^i \upharpoonright K(x): K(x) \rightarrow L$ sind p.w.v.

$$\Rightarrow [K(x):K] \geq m$$

Lemma
A20.11

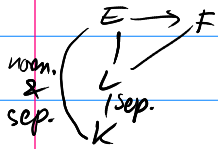
$$\text{Somit: } m \begin{pmatrix} 1 \\ K(x) \\ K \\ \vdots \\ K \end{pmatrix} \begin{matrix} L \\ \\ \\ \vdots \\ \\ \end{matrix}$$

$$\text{Also: } L = K(x).$$

$$\text{Wegen } \sigma(x^m) = (\sigma x)^m = (\xi x)^m = \underbrace{\xi^m}_{=1} x^m = x^m \quad \text{ist } x^m \in \text{Fix}(\sigma) = \text{Fix}(\langle \sigma \rangle) \\ = \text{Fix}(\text{Gal}(L|K)) \\ = K. \quad \square$$

$H_G \nearrow$

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



(1) $E|K$ normal und separabel.

(2) $\nexists F|L$ mit $F|K$ normal: $\exists \sigma: E \rightarrow F$ inj. über L .

Bew.: S. v. primitiven El. A20.11: $\exists \alpha \in L: L = K(\alpha)$

Sei f das Mipo von α über K , $E := \mathbb{Z}K$ von $f|K$

($\hookrightarrow$ Adjunktion aller Wurzeln von f)

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

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

Und: $F|K$ normal, $F|L \Rightarrow F \supseteq E$, d.h. (2).

Also: E änd. bestimmt. $\square$

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

Bem.: $\hookrightarrow$ Adjunktion aller Wurzeln von f , f Mipo von $x \in L$, alle $x \in L \setminus K$.

$\hookrightarrow$ mit jedem $x \in L$

liegt auch jede weitere "weitere Wurzel"/"Konjugierte" in E

24.10. Lemma: Die normale Hülle einer sep. Radikalerw. $L|K$ ist eine separable Radikalerw. $E|K$.

Bew.:

