Vorlesung Algebra

SoSe'21, hhu
K. Halupczok

Teil IV: und zurück (GALOISTHEORIE)

A22: Galoisgruppen

Stichworte: Galoisgruppe, galois, zyklische/abelsche Galoiserweiterung, Kreisteilungskörper, zyklische Gruppe der n-ten EWen in L, primitive n-te EW, Kreisteilungspolynom, endl. Erweiterungen eines endlichen Körpers sind zyklisch (galois)

22.1. Einleitung: Wir definieren die Galoisgruppe einer Körpererweiterung $L|K$. Ist die Erweiterung normal und separabel, nennen wir sie galois. Mit der zugehörigen Galoisgruppe (der Automorphismen über K) gelingt der Transfer gewisser Fragestellungen bei Körpererweiterungen in die Gruppentheorie zurück.

22.2. Def.: Sei $L|K$. Galoisgruppe von $L|K$: $\mathrm{Gal}(L|K) := \{\sigma \text{ Aut von } L|K,\ \sigma\restriction_K = \mathrm{id}_K\}$.

22.3. Def.: Endl. $L|K$ galois $:\Leftrightarrow$ $L|K$ normal und separabel.

22.4. Satz: $L|K$ galois $\Rightarrow$ $\#\,\mathrm{Gal}(L|K) = [L:K]$.

Bew.:
$$\begin{tikzcd} L \arrow[rr] \arrow[dr, dash, "\text{sep.}"'] & & L \arrow[dl, dash, "\text{norm.}"] \\ & K & \end{tikzcd}$$

Einbettungen: $\sigma: L \to L$ über K sind K-linear
$\ulcorner \sigma(ax) = \sigma(a)\sigma(x) = a\sigma(x) \lrcorner$,
also: inj. $\Leftrightarrow$ surj. $\Leftrightarrow$ σ Auto.

Lemma 20.11 $\Rightarrow$ $\#\,\mathrm{Gal}(L|K) = \#\Sigma = [L:K]$. $\square$

22.5. Bsp.: Sei $\mathrm{Char}\,K \neq 2$, $a \in K$ kein Quadrat.
Dann $T^2 - a \in K[T]$ irred. über K.
Sei x Wurzel in einer geeigneten Erw. von K.
$\Rightarrow$ $K(x)|K$ sep., da $2T$, T^2-a teilerfremd,
und normal, da $f := T^2 - a = (T-x)(T+x)$.
Daher: $K(x)|K$ galois.
Dann: $G := \mathrm{Gal}(K(x)|K) = \langle\sigma\rangle$ zyklisch der Ordnung 2.
$\ulcorner$Dabei, da $\sigma \neq \mathrm{id}_K$: $\sigma(a+bx) = a + b\sigma(x) = a - bx$.$\lrcorner$

22.6. **Bsp.:** Betr. $\mathbb{Q}(\sqrt[p]{2})$, $p \in \mathbb{N}$ prim, $p \geq 3$. $T^p - 2 \in \mathbb{Q}[T]$ Mipo von $\sqrt[p]{2}$.
$\mathbb{Q}(\sqrt[p]{2})$ ist nicht normal, s. Bsp. A19.9, also nicht galois $|\mathbb{Q}$.

22.7. **Bsp.:** Betr. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) | \mathbb{Q}$, ist sep. und normal (ZK von $(T^2-2)(T^2-3)$),
also galois. Ferner: $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$. Betr. Gruppenhom.:

$$\begin{tikzcd}[column sep=small] & K := \mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[dl, dash] \arrow[dr, dash] & \\ \mathbb{Q}(\sqrt{2}) \arrow[dr, dash] & & \mathbb{Q}(\sqrt{3}) \arrow[dl, dash] \\ & \mathbb{Q} & \end{tikzcd}$$

$$\tau : \mathrm{Gal}(K|\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\sqrt{2})|\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\sqrt{3})|\mathbb{Q})$$
$$\sigma \mapsto (\sigma \restriction \mathbb{Q}(\sqrt{2}), \sigma \restriction \mathbb{Q}(\sqrt{3})),$$

also: $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})|\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\sqrt{3})|\mathbb{Q}) \cong C_2 \times C_2$
nach Bsp. 22.5.

τ ist injektiv: $\left.\begin{array}{l} \sigma \restriction \mathbb{Q}(\sqrt{2}) = id \Rightarrow \sigma(\sqrt{2}) = \sqrt{2} \\ \sigma \restriction \mathbb{Q}(\sqrt{3}) = id \Rightarrow \sigma(\sqrt{3}) = \sqrt{3} \end{array}\right\} \Rightarrow \sigma = id.$

Somit: $\mathrm{Gal}(K|\mathbb{Q}) \cong C_2 \times C_2$.

22.8. **Bem.:** Ex. $L|\mathbb{Q}$ mit $\mathrm{Gal}(L|\mathbb{Q}) \cong G$ (vorgegeben) ? $\rightsquigarrow$ ungelöst!

22.9. **Def.:** Galoiserw. $L|K$ zyklisch (bzw. abelsch) $:\Leftrightarrow$ $\mathrm{Gal}(L|K)$ zyklisch (bzw. abelsch)

22.10. **Bsp.:** Sei $L|K$ der ZK eines sep. $f \in K[T]$,
$X := \{x_1, \dots, x_n\} \subseteq L$ die Menge der Wurzeln von f,
also $f = a \prod_{i=1}^{n} (T - x_i)$.
Dann: $G := \mathrm{Gal}(L|K)$ operiert auf X:

$$G \times X \to X$$
$$(\sigma, x) \mapsto \sigma x := \sigma(x).$$

Somit: $G \longrightarrow \mathrm{Perm}(X)$
$\sigma \longmapsto \sigma \restriction X$ ist inj. Gruppenhom., vgl. Bsp. A4.19,
inj., da $L = K(x_1, \dots, x_n)$.

22.11. **Def.:** Sei $L|K$ der ZK des sep. $f \in K[T]$, dann heißt $\mathrm{Gal}(L|K)$
die Galoisgruppe von f (bzw. G-Gr. der Gleichung $f = 0$).

22.12. **Bem.:** $\mathrm{Gal}(L|K)$ Galoisgruppe von $f \Rightarrow [L:K] = \#\mathrm{Gal}(L|K) \leq n!$, $n := \deg(f)$.

22.13. **Def.:** Ein Kreisteilungskörper der Ordnung n über K ist ein ZK von $T^n - 1 \in K[T]$.

22.14. **Bsp.:** Gelte $\operatorname{Char} K \nmid n$. Dann $(T^n-1)' = nT^{n-1} \neq 0$ teilerfremd zu T^n-1.
$\Rightarrow$ Der Kreisteilungskörper L (der Ordnung n über K) ist galois.

22.15 **Def.:** $E_n := \{x \in L;\ x \text{ Wurzel von } T^n - 1 \in K[T]\}$,
$x \in E_n$ heißt n-te Einheitswurzel in L, Kurz: n-te EW in L.

22.16. **Bem.:** * Dann: E_n zyklische Gruppe der Ordnung n:
$$\zeta^n = 1,\ \xi^n = 1 \Rightarrow \zeta^n \xi^n = (\zeta\xi)^n = 1.$$
* Betr.:
$$\begin{tikzcd} G = \mathrm{Gal}(L|K) \arrow[r] \arrow[dr, "\text{inj.}"'] & \mathrm{Perm}(E_n) \\ & \mathrm{Aut}(E_n) \arrow[u, phantom, "\cup\!|"] \end{tikzcd}$$
$\sigma \in G$
$\sigma|_{E_n}$ ist Auto der Gruppe E_n.
* Da $\mathrm{Aut}(E_n) \cong (\mathbb{Z}/(n))^\times$, wegen $\mathrm{End}(E_n) \cong \mathbb{Z}/(n)$,
ist G isomorph einer UG von $(\mathbb{Z}/(n))^\times$, d.h. insb. ist G abelsch.
* Für $K = \mathbb{Q}$ hat man "Gleichheit" [ohne Beweis], d.h. $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}) \cong (\mathbb{Z}/(n))^\times$
und $[\mathbb{Q}(\zeta):\mathbb{Q}] = \varphi(n)$ für ein erzeugendes El. ζ von $E_n|\mathbb{Q}$, etwa $\zeta := e^{\frac{2\pi i}{n}}$.

22.17. **Def.:** Die erzeugenden El. von E_n heißen primitive n-te Einheitswurzeln.
Das Mipo von $\zeta \in E_n$ über K, $\operatorname{Char} K \nmid n$, heißt n-tes Kreisteilungspolynom.

22.18 **Bsp.:** Sei $p \in \mathbb{N}$ prim, $K = \mathbb{F}_{p^m}$, $L|K$ die Erw. von K vom Grad n, ist galois.
Sei σ der Frobeniusautomorphismus von L, d.h. $\sigma x = x^p$.
Sei $\tau = \sigma^m \in \mathrm{Gal}(L|K)$: $\tau(x) = x^{p^m} = x$ für alle $x \in \mathbb{F}_{p^m} = K$.
$\Rightarrow \tau^n(x) = x^{p^{m\cdot n}} = x$ für alle $x \in L \cong \mathbb{F}_{p^{mn}}$, sei $q := p^m$.
Für $1 \leq i < n$: $\tau^i(x) = x^{q^i} \neq x$ für ein $x \in L$.
[Sonst hätte $T^{q^i} - T$ ja $\#L = q^n$ versch. Wurzeln.]
$\Rightarrow \tau \in \mathrm{Gal}(L|K)$ hat die Ordnung n
$\Rightarrow \mathrm{Gal}(L|K) = \langle \tau \rangle$ ist zyklisch.