Vorlesung Algebra

SoSe'21, hhu
K. Halupczok

Teil IV: und zurück (GALOISTHEORIE)

A23: Hauptsatz der Galoistheorie

Stichworte: Fixkörper, Zwischenkörper, symmetrische Polynome, elementarsymmetrische Funktionen, Hauptsatz der Galoistheorie: UGen der Galoisgruppen entsprechen genau den Zwischenkörpern der Körpererweiterung (und die NT entsprechen den normalen Zwischenkörpern), Anhang: Hauptsatz der Algebra als Anwendung des Hauptsatzes der Galoistheorie

---

23.1. Einleitung: Mit dem Fixkörperbegriff werden Eigenschaften der Galoisgruppe zurück auf Eigenschaften der zugehörigen Körpererweiterungen geführt. Wir zeigen den Hauptsatz der Galoistheorie, der die Verbindungen zwischen Körpererweiterungen und Gruppentheorie zusammenfasst.

23.2. Def.: Sei $L|K$ Galoiserw., Galoisgruppe sei G, $H \subseteq G$ UG, dann:
$E := Fix(H) := \{x \in L;\ \forall \sigma \in H: \sigma x = x\}$ heißt Fixkörper von H.

23.3. Bem.: E ist Zwischenkörper von $L|K$, d.h. $K \subseteq E \subseteq L$.

23.4. Satz: Sei G endl. UG der Automorphismengruppe eines Körpers L,
$K := Fix\, G$. Dann: $L|K$ endl. Galoiserw., $Gal(L|K) = G$.

Bew.: * Setze $n := \#G$, sei $x \in L$. Sei $x = x_1, x_2, \dots, x_m$ Aufzählung von $\{\tau x;\ \tau \in G\}$, dabei ist $m \le n$.

* Setze $f(T) := \prod_{i=1}^{m} (T - x_i)$, $f \in K[T]$, denn:
Für $\sigma \in G$: $\{\sigma x_1, \sigma x_2, \dots, \sigma x_m\} = \{x_1, \dots, x_m\}$, $\quad (\sigma x_i = (\sigma\tau)x_1)$
also: $f^\sigma = \prod_{i=1}^{m} (T - x_i)^\sigma = \prod_{i=1}^{m} (T - \sigma x_i) = f$.

* Resultat: $[K(x):K] \le n$ für alle $x \in L$.

* Sei $x \in L$ mit $[K(x):K]$ maximal.
Dann: $L = K(x)$. [Sonst: Sei $y \in L \setminus K(x) \Rightarrow K(x) \subsetneq K(x,y) = K(z)$ für ein $z \in L$ nach dem Satz vom primitiven Element A20.16. (denn $L|K$ ist separabel nach obigem), $\lightning$ zur Maximalität von $x \in L$.]

* Somit: $[L:K] \le n$. Da $G \subseteq Gal(L|K)$:
$n = \#G \le \#Gal(L|K) = [L:K] \le n \Rightarrow [L:K] = n$ und $Gal(L|K) = G$. □

23.5. **Anwendung:** Sei k Körper, $n \geq 1$, $k[X_1, \dots, X_n]$ Polynomring in $X_1, \dots, X_n$ über k.
Jedes $\sigma \in S_n$ def. einen Automorphismus

$$\bar{\sigma} : k[X_1, \dots, X_n] \longrightarrow k[X_1, \dots, X_n]$$
$$f(X_1, \dots, X_n) \mapsto f(X_{\sigma 1}, \dots, X_{\sigma n}).$$

23.6. **Def.:** f symmetrisch (es Polynom) $:\Leftrightarrow \forall \sigma \in S_n : \bar{\sigma}(f) = f$.

weiter 23.5: Sei $k(X_1, \dots, X_n) =: L$ der Quotientenkörper von $k[X_1, \dots, X_n]$,
der rationale Funktionenkörper in $X_1, \dots, X_n$ / k.
Seine El. sind von der Form $\frac{f(X_1, \dots, X_n)}{g(X_1, \dots, X_n)}$ mit $f, g \in k[X_1, \dots, X_n]$.

Jedes $\bar{\sigma}$ lässt sich eind. erweitern zu einem Auto $\tilde{\sigma} : L \to L$ vermöge

$$\tilde{\sigma}\left(\frac{f(X_1, \dots, X_n)}{g(X_1, \dots, X_n)}\right) := \frac{f(X_{\sigma 1}, \dots, X_{\sigma n})}{g(X_{\sigma 1}, \dots, X_{\sigma n})} = \frac{\bar{\sigma}(f(X_1, \dots, X_n))}{\bar{\sigma}(g(X_1, \dots, X_n))}.$$

Dann ist: $S_n \longrightarrow \mathrm{Aut}(L)$, $\sigma \mapsto \tilde{\sigma}$, ist inj. Gruppenhom.
Daher: Identifikation von S_n mit Bild in $\mathrm{Aut}(L)$.
Setze nun: $K := \mathrm{Fix}(S_n) \subseteq L$.
Nach Satz 23.4 ist $L|K$ galois, $[L:K] = \#S_n = n!$.
Sei $f(T) = (T - X_1) \cdot \dots \cdot (T - X_n) \in K[T]$, dann $f^{\sigma}(T) = f(T)$.
Ausmultiplizieren: $f = T^n - s_1 T^{n-1} + \dots + (-1)^n s_n$
mit $s_1 = X_1 + \dots + X_n$, $s_2 = \sum_{i<j} X_i X_j, \dots$, $s_n = X_1 \cdot \dots \cdot X_n$.

23.7. **Def.:** Allgemein: $s_j = \sum_{\nu_1 < \dots < \nu_j} X_{\nu_1} \cdot \dots \cdot X_{\nu_j}$ heißt die j-te elementarsymmetrische Funktion.

23.8. **Beh.:** $K = k(s_1, \dots, s_n)$.

Bew.: $L = k(X_1, \dots, X_n)$

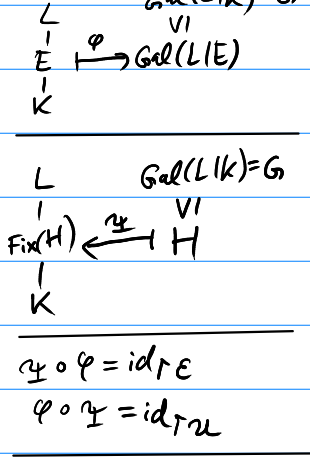
z.Z.: $\leq n!$

$|n!$
K
$|$
$k(s_1, \dots, s_n)$

Zeige nur: $[L : k(s_1, \dots, s_n)] \leq n!$:
L ist zK von f über $k(s_1, \dots, s_n)$,
$\deg f = n \Rightarrow [L : k(s_1, \dots, s_n)] \leq n!$.
Somit ist $[K : k(s_1, \dots, s_n)] = 1$, also $K = k(s_1, \dots, s_n)$. □

23.9. **Resultat:** Jede symmetrische rationale Funktion in $X_1, \dots, X_n$ ist rational in den n elementarsymmetrischen Funktionen.

23.10. **Hauptsatz der Galoistheorie:**



Sei $L|K$ endl. Galoiserw., $G = Gal(L|K)$. Dann gilt:

(1) $\mathcal{E} := \{E;\ E \text{ Zwischenkörper von } L|K\} \leftrightarrow \{H;\ H \leq G\ UG\} =: \mathcal{U}$

$\varphi: E \mapsto Gal(L|E)$

$Fix(H) \hookleftarrow H : \Psi$

sind zueinander inverse Bijektionen.

(2) $G \geq H$ UG ist NT $\Leftrightarrow$ $Fix(H) =: E$ ist normal $|K$.

Dann: $\boxed{Gal(E|K) \cong G/H}$.

Bew.: (1): * Sei $E \in \mathcal{E}$, zeige: $E \overset{!}{=} \Psi\circ\varphi(E) = Fix(Gal(L|E))$, denn:

$\#Gal(L:E) = [L:E] =: m \Rightarrow [L:Fix(H)] = m$ nach Satz 23.4.

Da $E \subseteq Fix(H)$, folgt $E = Fix(H)$.

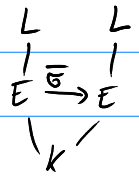
* Sei $H \in \mathcal{U}$, $E := Fix(H)$, $H' := Gal(L|E)$, zeige: $H \overset{!}{=} \varphi\circ\Psi(H) = H'$,

denn: $H \subseteq H'$ trivial. Ferner gilt $[L:E] = \#H$ nach Satz 23.4,

und: $\#H' = \#Gal(L|E) = [L:E] = \#H$, also $H = H'$.

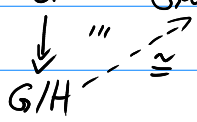
(2): „$\Leftarrow$": Sei $E|K$ normal. $\Phi: G \to Gal(E|K)$

$\sigma \mapsto \sigma|E$ ist Gruppenhomomorphismus,



$\ker\Phi = Gal(L|E) = H$, d.h. H ist NT in G.

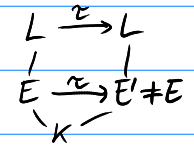
Φ ist surj. nach A19.6. [Fortsetzen von Körperiso.]



Hom.satz: $G/H \cong Gal(E|K)$.

„$\Rightarrow$": Sei $E|K$ nicht normal. Dann ex. $\tau \in G$: $E' := \tau E \neq E$.

Setze $H := Gal(L|E)$, $H' := Gal(L|E')$, also $H \neq H'$.



* Es gilt: $\tau H \tau^{-1} \overset{!}{=} H' \neq H$.

„$\subseteq$": Sei $\sigma \in H$, $x' \in E'$, $x' = \tau(x)$, $x \in E$.

$\Rightarrow \tau\sigma\tau^{-1}(x') = \tau\sigma(x) = \tau x = x' \Rightarrow \tau\sigma\tau^{-1} \in H'$.

„$\supseteq$": Ebenso: $\tau^{-1}H'\tau \subseteq H$.

Also: H kein NT. □

23.11. **Anhang:** Wir beweisen mit den Mitteln des Hauptsatzes der Galoistheorie 23.10 als Anwendung den

Hauptsatz der Algebra: $\mathbb{C} = \mathbb{R}(i)$ ist algebraisch abgeschlossen,

d.h. für jede endliche alg. Erw. $L \mid \mathbb{C}$ gilt $L = \mathbb{C}$.

Dies bedeutet, dass jede über $\mathbb{C}$ alg. Zahl z bereits in $\mathbb{C}$ liegt,

bzw. dass jedes Polynom $f \in \mathbb{C}[T]$ vom Grad ≥ 1 vollständig in Linearfaktoren zerfällt,

bzw. dass jedes Polynom $f \in \mathbb{C}[T]$ vom Grad ≥ 1 eine Nullstelle in $\mathbb{C}$ besitzt.

23.12 **Lemma:** $\mathbb{C}$ hat keine alg. Erw. vom Grad 2.

Bew.: Sei $L \mid \mathbb{C}$ alg. Körpererw., $[L : \mathbb{C}] = 2$.

Dann ex. $x \in L$ mit $L = \mathbb{C}(x)$ und $x^2 \in \mathbb{C}$,

somit gen. z.z.: Jedes $z \in \mathbb{C}$ hat Quadratwurzel in $\mathbb{C}$.

Dazu sei $z = a + ib \in \mathbb{C}$. Gesucht: $x + iy \in \mathbb{C}$ mit

$$a + ib = (x+iy)^2 = (x^2 - y^2) + 2ixy \iff x^2 - y^2 = a \wedge 2xy = b.$$

Fall 1: $b = 0$: Setzen $x = 0$ oder $y = 0$, je nachdem ob $a < 0$ oder $a \geq 0$.

Dann ist das Gleichungssystem lösbar.

Fall 2: $b \neq 0$: Erhalten $y = \frac{b}{2x}$, eingesetzt in $x^2 - y^2 = a$ liefert

$$x^2 - \frac{b^2}{4x^2} - a = 0 \iff 4(x^4 - ax^2 - \tfrac{1}{4}b^2) = 0 \iff (x^2 - \tfrac{a}{2})^2 - \frac{a^2+b^2}{4} = 0$$

$$\iff x^2 = \frac{a}{2} \pm \sqrt{a^2+b^2}, \text{ ist lösbar in } \mathbb{R} \text{ mit } x \neq 0. \quad \square$$

23.13. **Hauptsatz der Algebra:** Sei $\mathbb{C} := \mathbb{R}(i)$ mit $i^2 = -1$. Dann ist $\mathbb{C}$ alg. abg. (in 23.12)

Benutzen zum Beweis folgende Eigenschaften von $\mathbb{R}$: (i) Jedes $x \geq 0$ ist ein Quadrat (in $\mathbb{R}$),

(ii) Jedes $f \in \mathbb{R}[T]$ von ungeradem Grad hat eine Nullstelle in $\mathbb{R}$.

[Gilt wegen Vollständigkeit von $\mathbb{R}$ bzw. dem Zwischenwertsatz in $\mathbb{R}$, vgl. Analysis.]

Bew.: Sei $L \mid \mathbb{C}$ eine endl. alg. Erw., z.z.: $L \stackrel{!}{=} \mathbb{C}$.

Sei Ω (durch Vergrößern von L) die Erw. $\Omega \mid \mathbb{R}$ galois.

Setzen $G := \mathrm{Gal}(\Omega \mid \mathbb{R})$.

Haben nun gemäß des Hauptsatzes 23.10 der Galoistheorie

die Galois-"Korrespondenz" der Körpertheorie einerseits mit den Zwischenkörpern

von $\Omega \mid \mathbb{R}$ und der Galoisgruppe G mit den zugehörigen Untergruppen.

Situation:

L	e
$\vert$	$\vert$
$\mathbb{C}$	H'
$2\vert$	$\vert$
$\mathbb{R}$	G

Da $\#G$ Produkt der Körpergrade $[L:\mathbb{C}]$ und $[\mathbb{C}:\mathbb{R}]=2$, ist $\#G$ gerade, etwa $\#G = 2^a \cdot m$, m ungerade.
Sei $H \subseteq G$ eine 2-Sylowgruppe, d.h. eine UG mit 2^a vielen El.
Sei $K := \mathrm{Fix}(H)$.
Dann ist $[K:\mathbb{R}] = m$ ungerade.

L	e
$2^k\vert$	$\vert 2^a$
K	H
$m\vert$	$\vert 1$
$\mathbb{R}$	G

Sei $x \in K$, $f \in \mathbb{R}[T]$ das Mipo von $x \vert \mathbb{R}$, setzen $d := \deg(f)$.
Dann: $\mathbb{R} \subseteq \mathbb{R}(x) \subseteq K$
mit $[\mathbb{R}(x):\mathbb{R}] = d$ und $[K:\mathbb{R}] = m$, also gilt $d \mid m$,
d.h. d ist ungerade, nach (ii) folgt somit $d=1$ und $K=\mathbb{R}$,
da f außer $x \in K$ keine anderen Nullstellen hat.

Somit ist $G = H$ eine 2-Gruppe.
Damit ist auch $G' := \mathrm{Gal}(L \vert \mathbb{C}) \subseteq G$ eine 2-Gruppe.
Ann.: $G' \neq e$.
Nun enthält eine 2-Gruppe eine UG H' vom Index 2,
denn nach A8.11/12 ist eine Normalreihe aus Faktoren von Ordnung 2 enthalten,
d.h. ein Faktor G'/H' erfüllt $[G':H'] = \#(G'/H') = 2$.
Der zugehörige Zwischenkörper hat dann Grad 2 über $\mathbb{C}$,
↯ zu Lemma 23.12.
Also ist $G' = e$, d.h. $L = \mathbb{C}$. □