Proseminar Körpertheorie

6. Vortrag - Das Kernstück der Galoistheorie

Von: Nguyen Hoai Viet Dang

06.06.2013

Prof. K. Wingberg, K. Hübner

1. Hauptsatz – Galois-Korrespondenz

Satz 1.1:

Sei $K \subset L$ *eine endliche Erweiterung. Folgende Eigenschaften sind äquivalent:*

(i) $K \subset L$ *ist galoissch*

(ii) $K \subset L$ *ist separabel und jeder K-Homomorphismus von L in den algebraischen Abschluss hat Bildbereich L*

(iii) $K \subset L$ *ist separabel und jedes irreduzible Polynom in* $K[X]$ *mit Nullstellen in L zerfällt in L*

(iv) $\exists P \in K[X]$ *separabel, sodass* $K \subset L$ *Zerfällungskörper von P ist.*

Beweis:
Sei Ω *ein algebraischer Abschluss von L.*
(i)=>(ii): Sei $i_0 : L \to \Omega$ *die Inklusion von L in* Ω *. So gilt* $i_0(L) = L$
Jedes Element $\sigma \in Gal(L/K)$ *definiert einen K-Homomorphismus,* $i_0 \circ \sigma =: L \to \Omega$
Nach Satz 5.8 (Vortrag 5) gilt: $N \leq [L:K]$ *und* $N = [L:K]$ *<=> L/K separabel,*
wobei N die Anzahl der K-Homomorphismen von L nach Ω *ist.*
Nun gilt: N = #Gal(L/K) = [L:K]
=> $K \subset L$ *separabel und alle K-Homomorphismen haben die Form* $i_0 \circ \sigma$
Außerdem: $\forall i : L \to \Omega$ *gilt :* $i(L) = i_0(L) = L$
(ii)=>(i): Sei $K \subset L$ *separabel. Nach Satz 5.8: Es gibt [L:K] K-Homomorphismen von L nach* Ω *. Da das Bild der Homomorphismen gleich L ist, definieren sie eindeutige K-Automorphismen von L. Daher gilt:* $[L:K] \leq \#Aut(L/K)$.
Nach Proposition 5.2.2 (Vortrag 5) gilt zudem: $\#Aut(L/K) \leq [L:K]$
=> $\#Aut(L/K) = [L:K]$
=> $K \subset L$ *galoissch*

(ii)=>(iii): Sei P irreduzibles Polynom in $K[X]$ *mit Nullstelle w in L.*
Sei E = $K[w] \subset L$ *Untererweiterung von K durch diese Nullstelle erzeugt.*
Nach Satz von Kronecker: $\forall a \in \Omega$ *, mit a Nullstellen, gibt es eindeutige K-Homomorphismen* $\varphi : E \to \Omega$ *, sodass* $\varphi(w) = a$ *von P*
φ *lässt sich erweitern zu einem K-Homomorphismus* $\sigma : L \to \Omega$ *mit* $\sigma(w) = a$. *Da* $\sigma(L) = L$, *gilt* $a \in L$ *und somit zerfällt P in L.*

(iii)=>(iv): Seien $x_1,..,x_n \in L$, *sodass* $L = K[x_{1,..}, x_n]$. *Die Minimalpolynome* $P_i \in K[X]$ *von* x_i *sind irreduzibel und haben Nullstellen in L. Es folgt, dass sie in L zerfallen und, da* $K \subset L$ *separabel ist, einfache Nullstellen haben. Sei* $P = KgV(P_1,..,P_n)$. *P zerfällt in einfache Nullstellen in L.*

=> P ist separabel und L Zerfällungskörper von P

(iv)=>(ii): Sei L Zerfällungskörper von einem separablen Polynom P, also L/K Separabel. Seien $x_1,..,x_n$ *Nullstellen von P in L. Sei* $\sigma : L \to \Omega$ *K-Homomorphismus.*

$\sigma(x_1),..,\sigma(x_n)$ *sind wieder Nullstellen von P, gehören also zu L.*
$L = K[x_1,..,x_n]$, *also* $\sigma(L) \subset L$

Lemma 1.2 *(Artin's Lemma):*

Sei L ein Körper und G eine endliche Gruppe von Automorphismen von L.

$K := L^G = \{ x \in L \mid \forall \sigma \in G, \sigma(x) = x \}$ *heißt Fixkörper von L über G.*

Dann ist K ein Teilkörper von L, sodass [L:K] = #G.
Insbesondere ist die Erweiterung $K \subset L$ *galoissch mit Gruppe G.*

Beweis:

- *K ist Teilkörper von L, da alle* $\sigma \in G$ *Automorphismen, insbes. Homomorphismen sind.*
- *Annahme: [L:K] > #G. Betrachte L als K-Vektorraum.*
  => wir finden n = 1 + #G linear unabhängige Elemente $a_1,..,a_n$ *in L über K.*
  Betrachte das folgende Gleichungssystem mit #G linearen Gleichungen und n Unbekannten und Koeffizienten in L. (unterbestimmt)

  $\sum_{j=1}^{n} \sigma(a_j) \cdot x_j = 0, \ \sigma \in G.$ *Es gibt eine Lösung* $\begin{pmatrix} x_1 \\ . \\ x_n \end{pmatrix}$ *in* L^n *mit Einträgen unleich 0.*

  Wähle $m \in \mathbb{N}$ *minimal, sodass bis auf Umnummerieren:* $x_{1,..} x_m \neq 0, \ x_{m+1},..,x_n = 0$
  Wegen Linearität können wie zudem annehmen: $x_m = 1$.

  => $\sum_{j=1}^{m-1} \sigma(a_j) \cdot x_j + \sigma(a_m) = 0, \ \forall \sigma \in G$ *(*)*

  Für $\tau^{-1} \circ \sigma, \ \tau \in G$: $\sum_{j=1}^{m-1} \tau^{-1} \circ \sigma(a_j) \cdot x_j + \tau^{-1} \circ \sigma(a_m) = 0$. *Wende* τ *darauf an:*

  $\tau\left(\sum_{j=1}^{m-1} \tau^{-1} \circ \sigma(a_j) \cdot x_j + \tau^{-1} \circ \sigma(a_m)\right) = \tau(0) = 0$, *d.h.* $\sum_{j=1}^{m-1} \sigma(a_j) \cdot \tau(x_j) + \sigma(a_m) = 0$ *(**).*

  (**)-(*) $\left(\Rightarrow\right)$ $\sum_{j=1}^{m-1} \sigma(a_j) \cdot (\tau(x_j) - x_j) = 0$.

  => $(\tau(x_1) - x_1,..,\tau(x_2) - x_2, 0,..,0)$ *ist eine Lösung des Gleichungssystems*
  Da m minimal: $\tau(x_j) = x_j \ \forall j$ => $x_j \in K \ \forall j$

  => $\sum_{j=1}^{n} id(a_j) \cdot x_j = 0$ *hat eine nicht-triviale Lösung über K. Widerspruch:* $a_{1,..}, a_n$ *l.u.*

  => $[L:K] \leq \#G$, *insbesondere ist die Erweiterung* $K \subset L$ *endlich.*
  Offensichtlich gilt $G \subset Aut(L/K)$. *Nach Prop. 5.2.2 (Vortrag 5) gilt:*
  $\#Aut(L/K) \leq [L/K]$ *, also* $\#G \leq [L:K]$

  => *[L:K] = #G*

  => $K \subset L$ *galoissch und Gal(L/K) = Aut(L/K) = G*

Hauptsatz 1.3 *(Galois-Korrespondenz):*

Sei $K \subset L$ *eine endliche Erweiterung mit Galoisgruppe G = Gal(L/K).*

a) *Für jede Untergruppe* $H \subset G$ *ist die Menge* $L^H = \{x \in L \mid \forall \sigma \in H, \sigma(x) = x\}$ *ein Unterkörper von L, der K enthält. Ferner gilt:*

[L:K] = (G:H), wobei (G:H) := $\frac{\#G}{\#H}$ *(Index von H in G)*

b) *Für jeden Körper E mit* $K \subset E \subset L$ *ist die Erweiterung* $E \subset L$ *galoissch mit Galoisgruppe* $Gal(L/E) = \{\sigma \in Gal(L/K) \mid \forall x \in E, \sigma(x) = x\}$.

c) *Die Abbildungen* $\varphi : H \to L^H$ *und* $\gamma : E \to Gal(L/E)$ *definieren inklusionsumkehrende Bijektionen zwischen der Menge der Untergruppen in G und der Menge der Unterkörper von L, welche K enthalte, wobei die Bijektionen invers zueinander sind.*

Beweis:

a) *Sei* $H \subset G$ *Untergruppe*
$\overset{Artin's\ Lemma}{\Rightarrow}$ $L^H \subset L$ *Galoiserweiterung mit Galoisgruppe H.*
Es gilt: $K \subset L^H$, *da* $H \subset G$ *und alle Elemente aus K von G auf sich selbst abgebildet werden.*
Ferner gilt: $[L^H : K] = \frac{[L:K]}{[L:L^H]} = (G:H)$

b) *Sei E ein Unterkörper von L mit* $K \subset E \subset L$.
Da $K \subset L$ *galoissch ist, folgt nach Satz 1.1: L ist Zerfällungskörper eines separablen Polynoms* $P \in K[X]$, *dann ist L auch Zerfällungskörper von P über E, also ist* $E \subset L$ *galoissch.*
Die E-Automorphismen von L sind genau die K-Automorphismen von L, die Elemente aus E auf sich selbst schicken.
$\Rightarrow$ $Gal(L/E) = \{\sigma \in Gal(L/K) \mid \forall x \in E, \sigma(x) = x\}$

c) *Sei* $H \subset G$ *Untergruppe*
$\varphi(H) = L^H \overset{Artin's\ Lemma}{\Rightarrow}$ $L^H \subset L$ *Galoiserweiterung mit Galoisgruppe H, also*
$\gamma(L^H) = Gal(L/L^H) = H$
Sei $K \subset E \subset L$, *nach b):* $E \subset L$ *galoissch mit Gruppe Gal(L/E). Es gilt* $L^{Gale(L/E)} \supset E$.
Ferner: Setze H := Gal(L/E). $[L:L^H] = \#H = [L:E]$
$\Rightarrow$ $L^{Gale(L/E)} = E$, *also* $\gamma(E) = Gal(L/E)$. $\varphi(Gal(L/E)) = L^{Gal(L/E)} = E$

inklusionsumkehrend:

zz: $H \subset H' \Rightarrow L^{H'} \subset L^H$

Sei $x \in L^{H'}$

$\sigma(x) = x \quad \forall \sigma \in H'$

$\tau(x) = x \quad \forall \tau \in H \subset H'$

$\Rightarrow$ $x \in L^H$

zz: $E \subset E' \Rightarrow Gal(L/E')\ subset Gal(L/E)$

Sei $\sigma \in Gal(L/E')$

$\sigma(x) = x \quad \forall x \in E'$

$\sigma(y) = y \quad \forall E \subset E'$

$\Rightarrow$ $\sigma \in Gal(L/E)$

2. Die Galoisgruppe als Permutationsgruppe

Lemma 2.1: *Sei K ein Körper,* $P \in K[X]$ *separables Polynom und* $K \subset L$ *ein Zerfällungskörper von P. Sei* $R \subset L$ *die Menge der Nullstellen von P in L. Es gilt:*

$$\sigma(x) \in R \quad \forall \sigma \in Gal(L/K) \quad \text{für} \quad x \in R$$

Die Einschränkung von σ *auf* R *induziert eine Permutation von R und die Abbildung*

$$\varphi : Gal(L/K) \to \sigma(R) \quad (= \text{Gruppe der Permutationen der Menge } R)$$

ist ein injektiver Gruppenhomomorphismus.

Beweis:

- *Ist* $\sigma \in Gal(L/K)$ *und* $x \in L$, *so ist* $\sigma(P(x)) = P(\sigma(x))$
  Für $P(x) = 0$ *gilt also* $P(\sigma(x)) = 0$ => $\sigma(x) \in R$ *für* $x \in R$
- *Da jedes* $x \in R$ *wieder nach R abgebildet wird, ist* $G|_R : R \to R$ *injektiv und da R endlich ist, auch bijektiv.* $\sigma|_R$ *Ist also Permutation von R.*
  => $\varphi : Gal(L/K) \to \sigma(R)$, $\varphi(\sigma) = \sigma|_R$ *ist ein Gruppenhomomorphismus*
  $((\sigma\tau)|_R = \sigma|_R \tau|_R)$
- *Injektivität:*
  Sei $\sigma \in Gal(L/K)$, *sodass* $\forall x \in R, \sigma(x) = x$. *Es ist zu zeigen:* $\sigma = id$
  Sei $L^\sigma = \{a \in L \mid \sigma(a) = a\}$ *Untererweiterung von L. Da* L^σ *alle Nullstellen enthält und L nach Voraussetzung Zerfällungskörper von P ist*
  => $L^G = L$, *also* $\sigma(a) = a \quad \forall a \in L$
  => $\sigma = id$

Definition 2.2:
Sei G eine Gruppe und X eine Menge. Man bezeichnet eine Gruppenoperation von G auf X als transitiv (/die Gruppe operiert transitiv auf X), wenn es zu je zwei Elementen $x_1, x_2 \in X$ *ein* $g \in G$ *gibt, sodass* $g * x_1 = x_2$.

Satz 2.3: *Sei K ein Körper,* $P \in K[X]$ *separables Polynom und* $K \subset L$ *Zerfällungskörper von P.* $Gal(L/K)$ *operiert transitiv auf den Nullstellen von P <=> P irreduzibel in* $K[X]$ *ist.*

Beweis:
„=>“: Sei R die Menge der Nullstellen von P in L.
Ann: P ist nicht irreduzibel
=> $\exists$ *nicht-konstante Polynome* $Q, S \in K[X]$, *sodass* $P = QS$
Da P separabel ist, sind Q und S teilerfremd. Daher gilt $R = R_1 \dot\cup R_2$, *wobei* R_1 *die Nullstellen von Q und* R_2 *die Nullstellen von S enthält.* R_1 *und* R_2 *sind disjunkt und nicht-leer.*
Sei $x \in R_1$ *und* $\sigma \in Gal(L/K)$: $Q(\sigma(x)) = \sigma(Q(x)) = \sigma(0) = 0$, *also* $\sigma(x) \in R_1$
Insbesondere: $\sigma(x) \notin R_2$
=> *Für* $x_1 \in R_1$ *und* $x_2 \in R_2$: $\nexists \sigma \in Gal(L/K)$: $\sigma(x_1) = x_2$
=>*Widerspruch: Gal(L/K) transitiv*

„<=“: *Sei P irreduzibel und* $x, y \in R$

=> $K \subset K[x]$, $K \subset K[y]$ *sind einfache und von Nullstellen von P erzeugte Untererweiterungen von L. Nach Satz von Kronecker:* $\exists!$ *K-Hom.* $f: K[x] \to K[y]$, , *sodass* $f(x) = y$.

Da $[K[x]:K] =$ *grad*(P) $= [K[y]:K]$ *, ist f Isomorphismus*

=> *L ist Zerfällungskörper von P über zwei isomorphe Unterkörper* $K[x]$ *und* $K[y]$

Nach Satz 3.2 b) (Vortrag 4): f lässt sich zu einem K-Automorphismus $\sigma: L \to L$ *fortsetzen*

=> *Wie haben ein* $\sigma \in Gal(L/K)$ *gefunden mit* $\sigma(x) = y$.

Literatur:

*Chambert-Loir, Antoine: A Field Guide to Algebra, S*pringer 2000