

24. Script zur Vorlesung: Algebra (B III)

Prof. Dr. Salma Kuhlmann, Gabriel Lehericy, Simon Müller

WS 2016/2017: 10. Februar 2017

Beweis Fundamentalersatz der Galois Theorie

Sei E/F eine endliche Galoiserweiterung. Betrachte die Abbildungen

$$\Sigma \xrightarrow{\gamma} \Gamma$$

$$K \mapsto \text{Gal}(E/K) \quad (\leq \text{Gal}(E/F))$$

und $\Gamma \xrightarrow{i} \Sigma$

$$H \mapsto \text{Inv } H \quad (\subseteq E \text{ und } \supseteq F)$$

wobei $\Gamma :=$ die Menge der Untergruppen von $G := \text{Gal}(E/F)$ ist und $\Sigma :=$ die Menge der Zwischenkörper $F \subseteq K \subseteq E$ ist.

Wir behaupten $i \circ \gamma = \text{Id}$ und $\gamma \circ i = \text{Id}$, i.e. $\text{Gal}(E/\text{Inv } H) = H$ und $\text{Inv}(\text{Gal}(E/K)) = K$, das heißt $(\gamma \circ i)(H) = H$ und $(i \circ \gamma)(K) = K$.

Das ist aber die letzte Aussage in Satz 0.6 der letzten Vorlesung (weil H endlich ist), genauer:

- $H \leq G$, also $F := \text{Inv } G \subseteq \text{Inv } H$ und $K = \text{Inv } H$ ist eine Zwischenerweiterung $F \subseteq K \subseteq E$. Die Anwendung von Satz 0.6 mit H anstatt mit G liefert $\text{Gal}(E/\text{Inv } H) = H$. Also $|H| = |\text{Gal}(E/\text{Inv } H)| = [E : \text{Inv } H]$ (siehe Lemma 0.3, letzte Vorlesung)
- Sei nun K ein Unterkörper von E/F (i.e. $F \subseteq K \subseteq E$) und $H := \text{Gal}(E/K)$, dann ist $H \leq G (= \text{Gal}(E/F))$.

Nun ist E immer noch Zerfällungskörper über K von einem separablen Polynom (weil E über F so ist). Also liefert die Anwendung von Satz 0.6 für E und K

$$K = \text{Inv } H = \text{Inv}(\text{Gal}(E/K))$$

- (i) ist eine unmittelbare Folgerung der allgemeinen Eigenschaften: $H_1 \supseteq H_2 \Rightarrow \text{Inv } H_1 \subseteq \text{Inv } H_2$. Nun ist $\text{Inv } H_1 \subseteq \text{Inv } H_2$, dann ist $H_1 = \text{Gal}(E/\text{Inv } H_1) \supseteq \text{Gal}(E/\text{Inv } H_2) = H_2$.
- Die erste Aussage in (ii) haben wir schon bewiesen: $|H| = [E : \text{Inv } H]$. Wir berechnen $|G| = [E : F] = [E : \text{Inv } H][\text{Inv } H : F] = |H|[\text{Inv } H : F]$, aber auch $|G| = |H|[G : H]$ (vergleiche: $|G| = |H|[\text{Inv } H : F]$ und $|G| = |H|[G : H] \Rightarrow [G : H] = [\text{Inv } H : F]$). Dies ist die zweite Aussage in (ii).

Zu (iii):

Sei $H \in \Gamma$ und $K := \text{Inv } H$. Dann ist $\text{Inv } (\eta H \eta^{-1}) = \eta(K)$ (für $\eta \in G$), weil für alle ξ gilt:
 $\xi(k) = k \Rightarrow (\eta \xi \eta^{-1})(\eta(k)) = \eta(k)$.

Es folgt: $H \triangleleft G \Leftrightarrow \eta(K) = K$ für alle $\eta \in G$ (*)

(i.e. K ist (mengenweise) invariant). Nehmen wir nun an, dass $H \triangleleft G$. Aus (*) folgt, dass $\bar{\eta} := \eta|_K$ ein Automorphismus von K über F ist. Betrachte also nun den Homomorphismus

$$\begin{aligned} \text{Gal}(E/F) = G &\rightarrow \text{Gal}(K/F) \\ \eta &\mapsto \bar{\eta} \end{aligned}$$

und berechne das Bild \bar{G} und den Kern davon.

Bemerke, dass $\text{Inv } \bar{G} = F$ und $\bar{G} = \text{Gal}(K/F)$. Der Kern ist die Menge aller $\eta \in G$ mit $\eta|_K = \text{Id}$. Das heißt, dass der Kern genau $\text{Gal}(E/K) = H$ ist. Wir bekommen nun $\bar{G} = \text{Gal}(K/F) \simeq G/H$. Da $F = \text{Inv } \bar{G}$, K/F ist eine normale Erweiterung (Satz 0.6, 2., letzte Vorlesung).

Umgekehrt: Sei K/F normal. Sei $a \in K$ und $f(x) := \text{Min.Pol.}_{F,a}$. $f(x)$ zerfällt in Linearfaktoren über $K[x]$.

Dann ist $f(x) = (x - a_1)(x - a_2) \cdots (x - a_n)$ in $K[x]$ mit $a = a_1$.

Sei $\eta \in G$, dann ist $0 = \eta(f(a)) = f(\eta(a))$. Also ist $\eta(a)$ eine Nullstelle und somit existiert ein i mit $\eta(a) = a_i$. Insbesondere ist $\eta(a) \in K$.

Wir haben gezeigt: $\eta(K) \subseteq K$ für alle $\eta \in G$ und damit ist durch (*) $H := \text{Gal}(E/K) \triangleleft G$. \square