26. Script zur Vorlesung: Algebra (B III)

Prof. Dr. Salma Kuhlmann, Dr. Lorna Gregory, Katharina Dupont

WS 2012/2013: 7. Februar 2013

(WS 2015/2016: Korrekturen vom 28. Januar 2016)

Beweis Fundamentaler Satz der Galois Theorie (siehe Satz 0.8, 25. Vorlesung)
Sei E/F eine endliche Galoiserweiterung. Betrachte die Abbildungen

$$\begin{array}{cccc} & \Sigma & \xrightarrow{\gamma} & \Gamma \\ & K & \mapsto & \text{Gal } (E/K) \quad (\leq \text{Gal } (E/F)) \\ \text{und} & \Gamma & \to & \Sigma \\ & H & \mapsto & \text{Inv } H \qquad (\subseteq E \text{ und } \supseteq F) \end{array}$$

wobei $\Gamma :=$ die Menge der Untergruppen von $G :=$ 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. Gal $(E/\text{Inv } H) = H$ und Inv (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 25. Vorlesung (weil H endlich ist), genauer:

- $H \leq G$, also $F :=$ Inv $G \subseteq$ Inv H und $K =$ Inv H ist eine Zwischenerweiterung $F \subseteq K \subseteq E$. Die Anwendung von Satz 0.6 mit H anstatt mit G liefert Gal $(E/\text{Inv } H) = H$. Also $|H| = |\text{Gal } (E/\text{Inv } H)| = [E : \text{Inv } H]$ (siehe Lemma 0.3, 25. Vorlesung)

- Sei nun K ein Unterkörper von E/F (i.e. $F \subseteq K \subseteq E$) und $H :=$ Gal (E/K), dann ist $H \leq G (=$ 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 (Übungsblatt, Aufgabe 12.1): $H_1 \supseteq H_2 \Rightarrow$ Inv $H_1 \subseteq$ Inv H_2. Nun ist Inv $H_1 \subseteq$ Inv H_2, dann ist $H_1 =$ Gal $(E/\text{Inv } H_1) \supseteq$ 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: $|H|[\text{Inv } H : F]$ 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 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: $H \lhd G \Leftrightarrow \eta(K) = K$ für alle $\eta \in G$ $(*)$
(i.e. K ist (mengenweise) invariant). Nehmen wir nun an, dass $H \lhd G$. Aus $(*)$ folgt, dass $\overline{\eta} := \eta|_K$ ein Automorphismus von K über F ist. Betrachte also nun den Homomorphismus

$$\begin{array}{rccc} \text{Gal } (E/F) = & G & \to & \text{Gal } (K/F) \\ & \eta & \mapsto & \overline{\eta} \end{array}$$

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

Bemerke, dass Inv $\overline{G} = F$ und $\overline{G} = \text{Gal } (K/F)$. Der Kern ist die Menge aller $\eta \in G$ mit $\eta|_K = \text{Id}$. Das heißt, dass der Kern genau Gal $(E/K) = H$ ist. Wir bekommen nun $\overline{G} = \text{Gal } (K/F) \simeq G/H$. Da $F = \text{Inv } \overline{G}, K/F$ ist eine normale Erweiterung (Satz 0.6, 2., 25. Vorlesung).
Umgekehrt: Sei K/F normal. Sei $a \in K$ und $f(x) := Min.Pol._F a$. $f(x)$ 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 $(*)$ $H := \text{Gal } (E/K) \lhd G$. $\square$