24 Script zur Vorlesung: Algebra 1 (WiSe2020-2021)

Prof. Dr. Salma Kuhlmann

In diesem Skript werden wir (endliche) Galois Erweiterungen definieren und Charakterisieren, und den Hauptsatz der Galoistheorie aussagen und beweisen.

Sei E/F stets eine algebraische Körpererweiterung.

Definition 24.1. Die Körpererweiterung E/F heißt *separabel* falls für jedes $\alpha \in E$, das Minimalpolynom $m_{\alpha,F}(x)$ separabel ist.

Definition 24.2. Die Körpererweiterung E/F heißt *Galoiserweiterung* falls E/F endlich, normal und separabel ist.

Satz 24.3. Sei E/F eine Körpererweiterung. Die folgende Aussagen sind äquivalent:

(i) E ist der Zerfällungskörper eines separablen Polynoms $p(x) \in F[x]$.

(ii) $F = \text{Inv}\,(G)$ für eine endliche Teilgruppe $G \leq \text{Aut}(E)$.

(iii) E/F ist eine Galoiserweiterung.

Darüberhinaus gelten:

(a) sind E und F wie in (i) und $G = \text{Gal}\,(E/F)$ dann ist $F = \text{Inv}\,(G)$
d.h. $\text{Inv}\,(\text{Gal}\,(E/F)) = F$

(b) sind G und F wie in (ii) dann ist $G = \text{Gal}\,(E/F)$
d.h. $\text{Gal}\,(E/\text{Inv}\,(G)) = G$.

Beweis: (i)⇒(ii):

• Setze $F' := \text{Inv}\,(\text{Gal}\,(E/F))$. Dann ist E auch ein Zerfällungskörper von $p(x)$ über F'. Es gelten: $F \subseteq F'$ und $\text{Gal}\,(E/F) \geq \text{Gal}\,(E/F')$ (Proposition 23.4). Per Definition von F' ist auch $\text{Gal}\,(E/F) \leq \text{Gal}\,(E/F')$. Also ist $\text{Gal}\,(E/F) = \text{Gal}\,(E/F')$.

• Aus Lemma 23.5 folgen $[E : F] = |\text{Gal}\,(E/F)|$ und $[E : F'] = |\text{Gal}\,(E/F')|$, also $[E : F] = [E : F']$. Daher ist $[F'/F] = 1$ (s. Satz 10.11). Also $F = F'$ und somit gelten (a) und (ii).

(ii)⇒(iii):

• Nach Lemma 23.6 ist E/F endlich.

• Sei $\alpha \in E$. Sei $\{\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_m\}$ die Bahn von α unter der Wirkung $(\sigma, \alpha) \mapsto \sigma(\alpha)$ von G. Setze $g(x) = \prod_{i=1}^{m}(x - \alpha_i)$. Für alle $\sigma \in G$ gilt $\sigma(g)(x) = \prod_{i=1}^{m}(x - \sigma(\alpha_i)) = g(x)$ (weil σ die Elemente $\alpha_1, \ldots, \alpha_m$ permutiert). Also $g(x) \in F[x]$ (weil die Koeffiziente von g in $\text{Inv}\,(G)$ liegen).

Aus $g(\alpha) = 0$ und $g(x) \in F[x]$ folgt, dass das Minimalpolynom m_α von α über F das Polynom g teilt. Da (per Definition) g separabel und daher, ist auch m_α separabel. Es folgt, dass E/F separabel ist.

• Außerdem liegen alle Nullstellen von m_α in E. Daher ist E/F normal (E ist der Zerfällungskörper der Minimalpolynomen über F aller $\alpha \in E$).

(iii)⇒(i):

• E/F ist normal und endlich, also E ist der Zerfällungskörper von endlich vielen Polynomen $p_1, \ldots, p_n \in F[x]$. Ohne Einschränkung können wir annehmen, dass die p_i paarweise verschieden, normiert und irreduzibel über F sind. Somit ist jedes p_i das Minimalpolynom über F von einem $\alpha_i \in E$. Da E/F separable ist, ist jedes p_i separable. Da die p_i verschieden sind, haben sie auch keine gemeinsame Nullstelle. Das Produkt $p_1 \cdots p_n$ ist somit auch separabel (s. Definition 13.2) und E ist sein Zerfällungskörper. Dies zeigt (i).

• Zu (b). Sei $F = \text{Inv}\ (G)$ für eine endliche Gruppe $G \leq \text{Aut}(E)$. Lemma 23.6 liefert $[E : F] \leq |G|$. Da (i) gilt, Lemma 23.5 liefert, dass $|\text{Gal}\ (E/F)| = [E : F]$. Es gilt $G \leq \text{Gal}\ (E/F)$ (Proposition 23.4) und daraus folgt nun $G = \text{Gal}\ (E/F)$. □

Bemerkung 24.4. Die Erweiterung E/F ist normal wenn E enthält ein Zerfällungskörper für das Minimalpolynom m_α (von α über F) , für jedes $\alpha \in E$. Das heißt, jedes irreduzibles Polynom $p(x) \in F[x]$ das eine Nullstelle $\alpha \in E$ hat zerfällt als Produkt von linearen Faktoren in $E[x]$. Die Erweiterung ist normal und separable wenn jedes irreduzibles Polynom $p(x) \in F[x]$ das eine Nullstelle $\alpha \in E$ hat zerfällt als Produkt von verschiedenen linearen Faktoren in $E[x]$. ÜA

Satz 24.5 (Hauptsatz der Galoistheorie)**.** Sei E/F eine Galoiserweiterung. Setze $G := \text{Gal}\ (E/F)$. Seien Γ die Menge aller Teilgruppen $H \leq G$ und Σ die Menge aller Zwischenkörper K mit $F \subseteq K \subseteq E$. Die Abbildungen

$$\begin{aligned} \Gamma \to \Sigma, &\quad H \mapsto \text{Inv}\ (H) \\ \Sigma \to \Gamma, &\quad K \mapsto \text{Gal}\ (E/K) \end{aligned}$$

sind bijektiv und Inverse voneinander.
Darüberhinaus gelten die folgende Eigenschaften:

(i) $H_1 \supseteq H_2 \iff \text{Inv}\ (H_1) \subseteq \text{Inv}\ (H_2)$;

(ii) $|H| = [E : \text{Inv}\ (H)]$ und $[G : H] = [\text{Inv}\ (H) : F]$;

(iii) $H \trianglelefteq G \iff \text{Inv}\ (H)/F$ normal ist. In diesem Fall gilt $\text{Gal}\ (\text{Inv}\ (H)/F) \simeq G/H$.

Beweis:
Benenne die Abbildungen:

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

• Wir behaupten also dass

$$i \circ \gamma = \text{Id} \text{ und } \gamma \circ i = \text{Id}$$

d.h.

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

d.h.

$$(\gamma \circ i)(H) = H \text{ und } (i \circ \gamma)(K) = K\ .$$

Das ist aber gerade die letzte Aussage in Satz 24.3 (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 24.3 (b) (mit H anstatt mit G) liefert $\text{Gal}\,(E/\text{Inv } H) = H$. Es gilt auch $|H| = |\text{Gal}\,(E/\text{Inv } H)| = [E : \text{Inv } H]$ (s. Lemma 23.5). Das ist die erste Aussage in (ii).

- Sei nun $F \subseteq K \subseteq E$ und $H := \text{Gal}\,(E/K)$, dann ist $H \leq G$.
  Nun ist E immer noch Zerfällungskörper über K von einem separablen Polynom (‡) (ÜA).
  Also liefert die Anwendung von Satz 24.3 (a) für E und K

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

- (i) ist eine unmittelbare Folgerung der allgemeinen Eigenschaften:
  $H_1 \supseteq H_2 \Rightarrow \text{Inv } H_1 \subseteq \text{Inv } H_2$.
  Umgekehrt wenn $\text{Inv } H_1 \subseteq \text{Inv } H_2$ 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 gilt, für alle $\eta \in G$:

$$\text{Inv } (\eta H \eta^{-1}) = \eta(K)$$

[ÜA; für alle ξ gilt nämlich: $\xi(k) = k \Rightarrow (\eta\xi\eta^{-1})(\eta(k)) = \eta(k)$.]

Es folgt: $H \trianglelefteq G \Leftrightarrow \eta(K) = K$ für alle $\eta \in G$ (∗) (ÜA).

[i.e. K ist *mengenweise invariant*].

Nehmen wir nun an, dass $H \trianglelefteq G$. Aus (∗) folgt, dass $\overline{\eta} := \eta|_K$ ein Automorphismus von K über F ist. Betrachte also nun die Erweiterung K/F und den Homomorphismus

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

Wir bezeichnen $\nu(G) := \overline{G}$. Wir berechnen Bild(ν) und Kern(ν).

Bemerke dass ν surjective ist, also $\overline{G} = \text{Gal}\,(K/F)$. In der Tat, läßt sich jede $\tau \in \text{Gal}\,(K/F)$ zu eine $\eta \in \text{Gal}\,(E/F)$ fortsetzen. Das folgt aus (‡) und Satz 12.1 (ÜA).

Der Kern ist die Menge aller $\eta \in G$ mit $\eta|_K = \text{Id}$. Das heißt, dass der Kern ist $\text{Gal}\,(E/K)$, also $\ker \nu = H$, wegen (†). Wir bekommen nun $\overline{G} = \text{Gal}\,(K/F) \simeq G/H$ (s. Satz 16.11).
Der Fixkörper von $\overline{G}$ in K ist F (ÜA). Also ist K/F eine normale Erweiterung (Satz 24.3).

Umgekehrt: Sei K/F normal. Sei $a \in K$ und $f(x)$ sein Minimalpolynom, $f(x)$ 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 (∗) $H := \text{Gal}\,(E/K) \trianglelefteq G$. □