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

Prof. Dr. Salma Kuhlmann

Kapitel 4

EINFÜHRUNG IN DIE GALOISTHEORIE

In diesem Kapitel werden wir die basische Begriffe einführen, und die Eigenschaften von Galoiserweiterungen studieren. Wir werden zunächst den Hauptsatz der Galoistheorie beweisen, und danach einige erste Anwendungen vorzeigen (u.a. den Satz vom primitiven Element, den Fundamentalsatz der Algebra, sowie die Charakterisierung von auflösbaren Erweiterungen). In der Vorlesung B4 (Algebra 2 / algebraische Zahlentheorie) im Sommer Semester werden wir unser Studium der Galoistheorie und ihre Anwendungen vertiefen.

Im Skript 23 werden wir das notwendige Werkzeug für den Hauptsatz der Galoistheorie präsentieren. Wir werden zunächst in Proposition 23.4 eine Korrespondenz und ihre allgemeine Eigenschaften etablieren. Der Beweis davon ist routinemäßig. Anspruchsvoller ist es zu untersuchen, wann genau Mengengleichungen (anstatt Mengeninklusionen) gelten. Dafür werden wir am Ende des Skripts zwei Hilfslemmata beweisen. Im Skript 24 werden wir dann die Charakterisierung von Galoiserweiterungen beweisen.

§21: Die Galois Korrespondenz

Sei E/F stets eine Körpererweiterung.

Definition 23.1. Wir bezeichnen mit $\mathrm{Aut}(E)$ die Menge

$$\mathrm{Aut}(E) := \{\sigma \,;\, \sigma : E \to E, \sigma \text{ ist ein bijektive Körperhomomorphismus } \}$$

versehen mit der Verknüpfung $\circ$ (Komposition).
Sie ist tatsächlich eine Gruppe (ÜA), und heißt die *Automorphismengruppe von* E.

Definition 23.2. Die *Galoisgruppe von* E/F ist die Menge

$$\mathrm{Gal}(E/F) := \{\mu \in \mathrm{Aut}(E) \,;\, \mu(\alpha) \,=\, \alpha \;\forall\, \alpha \in F\}\,.$$

Sie ist tatsächlich eine Teilgruppe von $\mathrm{Aut}(E)$ (ÜA).

Definition 23.3. Sei $G \leq \mathrm{Aut}(E)$ eine Teilgruppe. Die Menge

$$\mathrm{Inv}(G) := \{a \in E \,;\, \sigma(a) = a \;\forall\, \sigma \in G\}$$

ist der *G-fixierte Teilkörper* von E oder der *Fixkörper* von G.
Sie ist tatsächlich ein Teilkörper von E (ÜA).

Proposition 23.4. Sei Γ die Menge aller Teilgruppen von $\mathrm{Aut}(E)$ und Σ die Menge aller Teilkörper von E. Die Abbildungen

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

haben folgende Eigenschaften:

1. $H_1 \leq H_2 \Rightarrow \mathrm{Inv}(H_1) \supseteq \mathrm{Inv}(H_2)$,
2. $F_1 \subseteq F_2 \Rightarrow \mathrm{Gal}(E/F_1) \geq \mathrm{Gal}(E/F_2)$,
3. $\mathrm{Inv}(\mathrm{Gal}(E/F)) \supseteq F$,
4. $\mathrm{Gal}(E/\mathrm{Inv}(H)) \supseteq H$.

Beweis: ÜA. ÜB.

Lemma 23.5. Sei E ein Zerfällungskörper eines separablen Polynoms $p(x) \in F[x]$. Dann

$$|\mathrm{Gal}(E/F)| = [E : F].$$

Beweis: Wir beweisen eine ähnliche Aussage wie im Beweis vom Satz 12.1; wir werden nämlich folgende Behauptung beweisen:

Sei $\tau: F \to F'$ ein Körperisomorphismus. Sei $p(x) \in F[x]$ separabel. Sei E ein Zerfällungskörper für $p(x)$ und E' ein Zerfällungskörper für $\tau(p)(x)$. Es gibt genau $[E : F]$ Fortsetzungen von τ zu einem Isomorphismus $\sigma: E \to E'$.

Wir führen einen Beweis (eine Aufzälung) per Induktion nach $[E : F]$ aus.
• Wenn $[E : F] = 1$ gilt die Behauptung offensichtlich.
• Sei nun $[E : F] > 1$ und sei $\alpha \in E \setminus F$ eine Nullstelle von $p(x)$ mit Minimalpolynom $m_\alpha(x)$. Sei β Nullstelle von $\tau(m_\alpha)(x)$. Sei

$$\tau_\beta : F(\alpha) \to F'(\beta)$$

der (eindeutige) Isomorphismus der τ durch $\tau_\beta(\alpha) = \beta$ fortsetzt, und sei

$$S_\beta := \text{ die Menge aller Isomorphismen } E \to E' \text{ die } \tau_\beta \text{ fortsetzen.}$$

Wir bemerken dass $S_\beta \cap S_{\beta'} = \varnothing$ wenn $\beta \neq \beta'$.
Der Körper E ist auch ein Zerfällungskörper von $p(x)$ über $F(\alpha)$ und E' ist ein Zerfällungskörper von $\tau_\beta(p)(x)$ über $F'(\beta)$ (s. Definition 11.10). Da $[E : F(\alpha)] < [E : F]$ (s. Satz 10.11), folgt aus der Induktionsvoraussetzung dass

$$|S_\beta| = [E : F(\alpha)].$$

Das Polynom $m_\alpha(x)$ teilt $p(x)$, daher ist $m_\alpha(x)$ separabel und somit ist $\tau(m_\alpha)(x)$ auch separabel (s. Definition 13.2). Es folgt, dass $\tau(m_\alpha)(x)$ genau $[F(\alpha) : F]$ verschiedene Nullstellen hat (s. Proposition 10.6).
Jede Fortsetzung $\sigma : E \to E'$ von τ bildet α auf eine Nullstelle $\beta := \sigma(\alpha)$ von $\tau(m_\alpha)(x)$ ab. Also ist die Einschränkung von σ auf $F(\alpha)$ gleich τ_β. Das heißt, $\sigma \in S_\beta$.

Also gibt es insgesamt genau $[E : F(\alpha)][F(\alpha) : F]$ Isomorphismen $\sigma : E \to E'$ die $\tau : F \to F'$ fortsetzen. Unsere Behauptung wurde hiermit bewiesen.
Die Aussage des Lemmas folgt nun, sobald wir $E = E'$, $F = F'$ und $\tau = \mathrm{id}_F$ setzen. □

Lemma 23.6. Sei $G \leq \mathrm{Aut}(E)$ eine endliche Teilgruppe und setze $F = \mathrm{Inv}(G) \subseteq E$. Dann gilt

$$[E : F] \leq |G|.$$

Beweis: Seien $n = |G|$ und $G = \{\mu_1 = 1, \mu_2, \ldots, \mu_n\}$. Wir werden zeigen dass jede Menge mit $m > n$ Elementen aus E linear abhängig über F ist.

Seien $u_1, \ldots, u_m \in E$. Betrachte folgendes homogenes Gleichungssystem in den Variablen $x_1, \ldots, x_m$

$$\sum_{j=1}^{m} \mu_i(u_j)x_j = 0, \quad 1 \leq i \leq n. \tag{1}$$

Nach [Gesamtscript LA I (2019-2020); Korollar 7.2], hat das System (1) eine nichttriviale Lösung. Sei $(b_1, \ldots, b_m)$ eine nichttriviale Lösung mit der kleinsten Anzahl von $b_j \neq 0$. Nach Umbenennung der Variablen kann man annehmen, dass $b_1 \neq 0$. Weiter, nach Multiplikation mit b_1^{-1} können wir auch annehmen, dass $b_1 = 1$.

Nun zeigen wir per Widerspruch, dass $b_j \in F$ für alle $j = 1, \cdots, m$. Ohne Einschränkung können wir annehmen, dass $b_2 \notin F$ und $\mu_k(b_2) \neq b_2$ für ein $k \in \{1, \cdots, n\}$. Wenn wir μ_k auf (1) anwenden finden wir

$$\sum_{j=1}^{m} (\mu_k\mu_i)(u_j)\mu_k(x_j) = 0, \quad 1 \leq i \leq n. \tag{2}$$

Da $\mu_k\mu_1, \ldots, \mu_k\mu_n$ eine Permutation von $\mu_1, \ldots, \mu_n$ ist, folgt dass (1) und (2) äquivalent sind und

$$(\mu_k(1), \mu_k(b_2), \ldots, \mu_k(b_m)) = (1, \mu_k(b_2), \ldots, \mu_k(b_m))$$

auch eine Lösung von (1) ist. Daher ist auch

$$(0, b_2 - \mu_k(b_2), \ldots, b_m - \mu_k(b_m))$$

auch eine Lösung. Diese Lösung ist nichttrivial weil $b_2 \neq \mu_k(b_2)$, hat aber mehr nulle Einträge als $(b_1, \ldots, b_m)$. Dies widerspricht die Wahl von $(b_1, \ldots, b_m)$.
Es folgt, dass $b_j \in F$ für alle $j = 1, \cdots, m$. Die erste Gleichung vom (1) (mit $\mu_1 = 1$) ergibt

$$\sum_{j=1}^{m} b_j u_j = 0.$$

Somit sind $u_1, \ldots, u_m$ linear abhängig über F. □