Ein Crashkurs in Galoistheorie

Lukas-Fabian Moser, SS 2013

Wir setzen die Begriffe eines Körpers und einer (algebraischen) Körpererweiterung und des Grades einer endlichen Körpererweiterung voraus. **Außerdem wollen wir zur Vereinfachung vereinbaren, daß wir unter einem Körper stets einen Teilkörper von $\mathbb{C}$ verstehen wollen.** (Wir kennzeichnen aber die Stellen, an denen der Verzicht auf diese Annahme die Theorie komplizierter machen würde.)

Besonders übersichtliche Beweise beim Aufbau der Theorie bekommt man, wenn man den folgenden Satz als allererstes beweist (in vielen modernen Lehrbüchern wird er stattdessen ans Ende gestellt und aus dem Hauptsatz der Galoistheorie gefolgert):

Satz (Satz vom Primitiven Element)**.** *Ist $K \subset L$ eine endliche Erweiterung, so gibt es ein $\alpha \in L$ mit $L = K(\alpha)$.*[1]

Beweisskizze. Man zeigt die Aussage zuerst für Erweiterungen der Form $L = K(a, b)$ und beweist dazu, daß es ein $\lambda \in K$ gibt mit $K(a, b) = K(a + \lambda b)$ – genau gesagt funktioniert jedes λ, das nicht zufällig mit einer der Zahlen

$$\frac{a_i - a_j}{b_r - b_s} \in \mathbb{C}$$

übereinstimmt, wobei $a_1, \dots, a_n$ die komplexen Nullstellen des Minimalpolynoms von a über K und $b_1, \dots, b_m$ die Nullstellen des Minimalpolynoms von b über K sind.[2]

Für den allgemeinen Fall $L = K(a_1, \dots, a_n)$ schreibt man nun $L = K(a_1, \dots, a_{n-2})(a_{n-1}, a_n)$ und verwendet den schon bewiesenen Fall, um ein Induktionsargument zu ermöglichen. □

Zerfällungskörper und normale Erweiterungen

Definition (Zerfällungskörper)**.** Es sei $K \subset \mathbb{C}$ ein Körper und $F \in K[X]$ ein beliebiges Polynom. Der *Zerfällungskörper* von F über K ist der Körper $K(a_1, \dots, a_n)$, wobei $a_1, \dots, a_n \in \mathbb{C}$ die Nullstellen von F sind.[3]

[1] Will man in größtmöglicher Allgemeinheit arbeiten, so muß man in Charakteristik > 0 für die Gültigkeit des Satzes vom Primitiven Element annehmen, daß die Erweiterung L/K separabel ist.

[2] Details finden sich etwa in Cox, Galois Theory, Beweis von Theorem 5.4.1.

[3] Da wir ausdrücklich stets Teilkörper von $\mathbb{C}$ betrachten, können wir anstatt von „einem“ von „dem“ Zerfällungskörper sprechen.

Definition (Normale Erweiterung)**.** Eine algebraische Körpererweiterung $K \subset L$ heißt *normal*, wenn gilt: Ist $F \in K[X]$ irreduzibel, und besitzt F eine Nullstelle in L, so liegen *alle* (komplexen) Nullstellen von F in L.

Satz. *Ist L der Zerfällungskörper eines Polynoms $F \in K[X]$ über K, so ist die Erweiterung L/K normal. Umgekehrt entsteht jede endliche normale Erweiterung von K als Zerfällungskörper eines Polynoms aus $K[X]$.*

Beweisskizze. Es sei L der Zerfällungskörper von $F \in K[X]$ über K, also $L = K(a_1, \ldots, a_n)$, wobei a_i die Nullstellen von F sind. Es sei $G \in K[X]$ ein irreduzibles Element mit einer Nullstelle $b \in L$. Wir müssen zeigen, daß jede weitere komplexe Nullstelle b' von G ebenfalls in K liegt. Zum Beweis konstruiert man einen Körperhomomorphismus $K(a) \to \mathbb{C}$ mit $b \mapsto b'$, der auf K die Identität ist. Da $K(a) \subset L$ ist, kann man diesen Homomorphismus (nach einem Satz über die Fortsetzbarkeit von Körperhomomorphismen) fortsetzen zu einem Homomorphismus $L \to \mathbb{C}$. Aber jeder Körperhomomorphismus muß Nullstellen von F wieder auf Nullstellen von F abbilden, d.h. die a_i landen wieder in L und damit (wegen $L = K(a_1, \ldots, a_n)$) sogar ganz L. Das zeigt $b' \in L$.

Ist umgekehrt die Erweiterung L/K normal, so schreibe $L = K(a)$ nach dem Satz vom primitiven Element. Das Minimalpolynom F von a über K besitzt eine Nullstelle in L, und da die Erweiterung normal ist, liegen *alle* seine Nullstellen $a_1 = a, a_2, \ldots, a_n$ in L. Damit gilt sogar $L = K(a_1, \ldots, a_n)$, d.h. L ist der Zerfällungskörper von F. □

Definition (Galoiserweiterung)**.** Eine endliche, normale Körpererweiterung heißt *Galoiserweiterung* (oder *galoissch*).[4]

Der Satz besagt also, daß Galoiserweiterungen genau die Zerfällungskörper von Polynomen sind.

Galoisgruppen und der Hauptsatz der Galoistheorie

Es sei $K \subset L$ eine endliche Körpererweiterung.

Definition (K-Automorphismen)**.** Ein *K-Automorphismus* von L ist eine Abbildung $\sigma : L \to L$ mit $\sigma|_K = \mathrm{id}_K$, die Summen und Produkte erhält.

Jeder K-Automorphismus ist automatisch eine bijektive Abbildung.

Definition. Die *Galoisgruppe* der Erweiterung L/K ist die Menge $\mathrm{Gal}(L/K)$ aller K-Automorphismen von L.

$\mathrm{Gal}(L/K)$ ist eine Gruppe mit der Komposition von Abbildungen als Verknüpfung.

Zentral in der Galoistheorie ist das folgende Lemma, das man als eine Verbesserung der Normalitätseigenschaft für Galoiserweiterungen interpretieren kann:

[4] Würden wir nicht in $\mathbb{C}$, also insbesondere in Charakteristik 0 arbeiten, so wäre hier zusätzlich die sogenannte Separabilität der Erweiterung in die Definition aufzunehmen.

Lemma. *Es sei $K \subset L$ eine Galoiserweiterung, $F \in K[X]$ irreduzibel und $a \in L$ eine Nullstelle von F. Ist b eine weitere Nullstelle von F, so gibt es ein $\sigma \in \mathrm{Gal}(L/K)$ mit $\sigma(a) = b$.*

Beweisskizze. Man konstruiert nun zuerst einen K-Homomorphismus $\sigma_0 : K(a) \to \mathbb{C}$ mit $\sigma_0(a) = b$. Da L/K normal ist, ist $b \in L$ und damit $\sigma_0(K) \subset L$. Diese Abbildung σ kann man nun, wieder nach dem Satz über die Fortsetzbarkeit von Körperhomomorphismen, fortsetzen zu einem K-Automorphismus $\sigma : L \to L$. □

Satz. *Es ist stets $|\mathrm{Gal}(L/K)| \leqslant [L : K]$, und es gilt Gleichheit genau dann, wenn L/K eine Galoiserweiterung ist.*

Beweisskizze. Schreibe $L = K(a)$ nach dem Satz vom primitiven Element, und es sei $F \in K[X]$ das Minimalpolynom von a. Die Körperhomomorphismen $K(a) \to \mathbb{C}$, die auf K die Identität sind, entsprechen nun eindeutig den Nullstellen von F; ihre Anzahl ist genau $\deg F = [L : K]$ (denn Minimalpolynome besitzen keine doppelten Nullstellen[5]).

Gleichheit gilt genau dann, wenn jeder Körperhomomorphismus $K(a) \to \mathbb{C}$, der auf K die Identität ist, in Wirklichkeit ein K-Automorphismus von $K(a)$ ist, wenn also sein Bild in $K(a)$ liegt. Das ist genau dann der Fall, wenn jede Nullstelle von F in $K(a) = L$ liegt, also genau dann, wenn L der Zerfällungskörper von F ist, und dies ist genau dann der Fall, wenn die Erweiterung normal (also Galoissch) ist, siehe den Beweis des letzten Satzes. □

Ist $K \subset M \subset L$ ein Zwischenkörper, so ist $\mathrm{Gal}(L/M)$ eine Teilmenge (und sogar eine Untergruppe) von $\mathrm{Gal}(L/K)$. Umgekehrt kann man aus einer Untergruppe der Galoisgruppe einen Zwischenkörper der Erweiterung erhalten:

Definition (Fixkörper)**.** Ist $H \subset \mathrm{Gal}(L/K)$ eine Untergruppe, so nennt man

$$L^H := \{x \in L \,|\, \sigma(x) = x \text{ für alle } \sigma \in H\}$$

den *Fixkörper* von H.

Es gilt stets $K \subset L^H \subset L$, und L^H ist tatsächlich ein Körper (also ein Zwischenkörper der Erweiterung L/K).

Satz (Hauptsatz der Galoistheorie)**.** *Die Erweiterung L/K sei Galoissch und $G := \mathrm{Gal}(L/K)$. Dann sind die oben definierten Abbildungen zwischen der Menge der Untergruppen von G und der Menge der Zwischenkörper von L/K, also*

$$\begin{aligned} \{M \,|\, K \subset M \subset L \textit{ Zwischenkörper}\} &\rightleftarrows \{H \,|\, H \subset G \textit{ Untergruppe}\}, \\ M &\mapsto \mathrm{Gal}(L/M), \\ L^H &\hookleftarrow H \end{aligned}$$

sind invers zueinander und damit insbesondere bijektiv. Außerdem sind beide inklusionsumkehrend.

Ist ferner $K \subset M \subset L$ ein Zwischenkörper und $H = \mathrm{Gal}(L/M)$ die zugehörige Untergruppe, so gilt:

[5] Dies ist die Separabilität von irreduziblen Polynomen, die in Charakteristik 0 stets gilt.

i) Die Erweiterung L/M ist Galoissch mit Galoisgruppe H. Insbesondere gilt $[L : M] = |H|$ und deswegen $[M : K] = [G : H]$.

ii) Die Erweiterung M/K ist genau dann Galoissch, wenn $H \subset G$ ein Normalteiler ist, und dann ist

$$G/H \to \mathrm{Gal}(M/K)$$
$$[\sigma] \mapsto \sigma|_M$$

ein (wohldefinierter) Isomorphismus von Gruppen.

Beweisskizze. Die Zusatzaussage i) ist am einfachsten zu beweisen: Ist L Galoissch über K, also Zerfällungskörper eines Polynoms $F \in K[X]$, so ist L auch Zerfällungskörper des gleichen Polynoms über M, also ist L/M Galoissch. Nach dem letzten Satz folgt daraus $[L : M] = |\mathrm{Gal}(L/M)|$; die zweite Beziehung $[M : K] = [G : \mathrm{Gal}(L/M)]$ folgt nun aus dem Gradsatz und dem Satz von Lagrange.

Direkt anhand der Definitionen kann man nachrechnen, daß $M \subset L^{\mathrm{Gal}(L/M)}$ und $H \subset \mathrm{Gal}(L/L^H)$ gilt. Wesentlich schwieriger (und für den Rahmen dieses Seminars zu umfangreich) ist der Nachweis, daß beide Inklusionen sogar Gleichheiten sind.

Zum Beweis der Zusatzaussage ii) zeigt man zunächst, daß M genau dann Galoissch über K ist, wenn $\sigma(M) = M$ für jedes $\sigma \in G$ gilt. Aber es ist $M = L^H$ und deswegen, wie man direkt nachrechnen kann, $\sigma(M) = L^{\sigma H \sigma^{-1}}$; wegen der Korrespondenz von Untergruppen und Zwischenkörpern ist damit die Aussage $\sigma(M) = M$ äquivalent zu $\sigma H \sigma^{-1} = H$, und daß dies für alle $\sigma \in G$ gilt, ist genau die Definition eines Normalteilers.

Sei nun M/K Galoissch. Wegen $\sigma(M) = M$ für alle $\sigma \in G$ ist dann die Abbildung $\mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$, $\sigma \mapsto \sigma|_M$, ein wohldefinierter Gruppenhomomorphismus. Er ist surjektiv nach dem Satz über die Fortsetzbarkeit von Körperhomomorphismen, und sein Kern ist nach Definition genau $\mathrm{Gal}(L/M) = H$. Nach dem Homomorphiesatz induziert er damit einen Isomorphismus $G/H \to \mathrm{Gal}(M/K)$, wie behauptet. □

Odds and ends

Außerdem wird gelegentlich der folgende Begriff benötigt:

Definition (Galoisscher Abschluß)**.** Ist L/K eine endliche Körpererweiterung, so versteht man unter einem *Galoisschen Abschluß von L über K* eine (endliche) Erweiterung $L \subset \widetilde{L}$ mit der Eigenschaft: $\widetilde{L}/K$ ist Galoissch, und für keinen echten Zwischenkörper $L \subset M \subsetneq \widetilde{L}$ ist M/K Galoissch.

Satz. *Ist L/K eine endliche Körpererweiterung, so existiert ein Galoisscher Abschluß von L über K, und er ist (als Teilkörper von $\mathbb{C}$) eindeutig bestimmt.*[6]

Beweis der Existenz. Der wohl einfachste Existenzbeweis greift auf den Satz vom Primitiven Element zurück: Wähle $\alpha \in L$ mit $L = K(\alpha)$. Es sei $F \in K[X]$ das Minimalpolynom von α über K. Definiere dann $\widetilde{L}$ als den Zerfällungskörper von F über K. Dann ist $L \subset \widetilde{L}$ wegen $\alpha \in \widetilde{L}$, und $\widetilde{L}$ ist als Zerfällungskörper Galoissch über K. Wäre nun ein echter Teilkörper $L \subset M \subsetneq \widetilde{L}$ Galoissch über K, so enthielte er (als normale Erweiterung von K) mit α auch automatisch den Zerfällungskörper von F über K, also $\widetilde{L}$ – Widerspruch. □

[6] Auch dieser Satz gilt im Allgemeinen nur für *separable* Erweiterungen.