Prof. Dr. H. Brenner **Osnabrück SS 2011**

Körper- und Galoistheorie

Vorlesung 21

DEFINITION 21.1. Es sei $K \subseteq L$ eine algebraische Körpererweiterung. Man nennt einen Körper N mit $L \subseteq N$ eine *normale Hülle* von L über K, wenn N der gemeinsame Zerfällungskörper aller Minimalpolynome von Elementen aus L ist.

LEMMA 21.2. *Sei $K \subseteq L$ eine endliche Körpererweiterung. Dann existiert die normale Hülle $L \subseteq N$.*

Beweis. Es sei $L = K(x_1, \ldots, x_n)$ und seien $P_1, \ldots, P_n$ die zugehörigen Minimalpolynome. Wir setzen $P = P_1 \cdots P_n$, und es sei N der Zerfällungskörper von P über L. Nach Satz 14.5 ist die Körpererweiterung $K \subseteq N$ normal. □

Auflösbare Körpererweiterungen

Wir kommen nun zu einer Ausgangsfrage zurück, nämlich zur Frage, ob man für jedes gegebene Polynom $P \in \mathbb{Q}[X]$ eine Kette von einfachen Radikalerweiterungen $\mathbb{Q} \subseteq K_1 \subseteq \ldots \subseteq K_n = K$ finden kann, so dass K die Nullstellen von P enthält. Dies ist die körpertheoretische Variante der Frage, ob es entsprechend zur Lösungsformel von Cardano auch für höhere Grade eine Lösung mit Radikalen gibt. Diese Fragestellung führt zu den folgenden Begriffen.

DEFINITION 21.3. Eine Körpererweiterung $K \subseteq L$ heißt *auflösbar*, wenn es eine Radikalerweiterung $K \subseteq M$ mit $L \subseteq M$ gibt.

DEFINITION 21.4. Es sei K ein Körper und $F \in K[X]$ ein Polynom. Man sagt, dass das Polynom F *auflösbar* ist (bzw., dass die Gleichung $F(x) = 0$ *auflösbar* ist), wenn die Körpererweiterung $K \subseteq Z(F)$ auflösbar ist.

Wir erinnern daran, dass eine Radikalerweiterung aus einer Kette von einfachen Radikalerweiterungen besteht, wobei eine einfache Radikalerweiterung durch die Adjunktion einer gewissen Wurzel eines Elements gegeben ist.[1] Eine Radikalerweiterung $K \subseteq L$ nennt man eine *m-Radikalerweiterung*, wenn es eine Körperkette aus einfachen Radikalerweiterungen $L_{i+1} = L_i(x_i)$ gibt, wobei die Beziehung $x_i^m \in L_i$ gilt. Jede Radikalerweiterung ist eine *m-Radikalerweiterung* für viele m, beispielsweise kann man jedes gemeinsame

[1] Man beachte, dass eine einfache Radikalerweiterung *nicht* das gleiche ist wie eine Radikalerweiterung, die zugleich eine einfache Körpererweiterung ist.

Vielfache der Einzelexponenten der beteiligten einfachen Radikalerweiterungen nehmen. Ein solches m hat (ähnlich wie der Exponent bei Kummererweiterungen) lediglich die Funktion, gewisse numerische Daten durch eine „gemeinsame Schranke“ zu kontrollieren.

LEMMA 21.5. *Es sei $K \subseteq L$ eine m-Radikalerweiterung. Dann ist auch die normale Hülle N von L eine m-Radikalerweiterung von K.*

Beweis. Es sei eine Körperkette aus einfachen Radikalerweiterungen gegeben, also

$$K = L_0 \subseteq L_1 \subseteq \ldots \subseteq L_n = L$$

mit $L_{i+1} = L_i(x_i)$ und $x_i^m \in L_i$. Wir zeigen durch Induktion über n, dass die normale Hülle von L über K ebenfalls eine m-Radikalerweiterung ist. Bei $n = 0$ ist nichts zu zeigen. Wir nehmen also an, dass die Aussage schon für kleinere Zahlen $n' < n$ bewiesen sei. Es sei $L \subseteq N$ die normale Hülle, die die normale Hülle N_{n-1} von L_{n-1} enthält. Nach Induktionsvoraussetzung ist $K \subseteq N_{n-1}$ eine m-Radikalerweiterung. In N_{n-1} zerfallen die Minimalpolynome der x_i, $i \leq n-2$, und in N zerfallen die Minimalpolynome der x_i, $i \leq n-1$. Daher ist $N = N_{n-1}(\alpha_1, \ldots, \alpha_k)$, wobei die α_j die Nullstellen des Minimalpolynoms von x_{n-1} sind. Wegen $x_{n-1}^m = a_{n-1} \in L_{n-1}$ sind diese α_j auch Nullstellen des Polynoms $X^m - a_{n-1}$. □

Wir kommen nun zur gruppentheoretischen Charakterisierung von auflösbaren Körpererweiterungen. Dabei beschränken wir auf Charakteristik null. Dies sichert, dass es zu jeder Zahl n primitive n-te Einheitswurzeln in einem Erweiterungskörper gibt. Durch die Hinzunahme von Einheitswurzeln können wir auf eine Situation hin transformieren, in der wir mittels Kummertheorie aus der Kommutativität von gewissen Galoisgruppen auf die Existenz von Wurzeln schließen können.

SATZ 21.6. *Es sei K ein Körper der Charakteristik 0 und sei $K \subseteq L$ eine Galoiserweiterung. Dann ist die Körpererweiterung $K \subseteq L$ genau dann auflösbar, wenn ihre Galoisgruppe $\mathrm{Gal}\,(L|K)$ auflösbar ist.*

Beweis. Es sei zuerst die Körpererweiterung $K \subseteq L$ auflösbar, und zwar sei $L \subseteq M$ eine Körpererweiterung derart, dass $K \subseteq M$ eine Radikalerweiterung ist. Es sei m dabei ein gemeinsamer „Radikalexponent“ der einfachen Radikalerweiterungen. Da wir in Charakteristik null sind, können wir zu M eine m-te primitive Einheitswurzel ζ adjungieren und erhalten eine Radikalerweiterung $K \subseteq M' = M(\zeta)$. Wir ersetzen M' durch seine normale Hülle M'', die nach Lemma 21.5 ebenfalls eine m-Radikalerweiterung von K ist. Da wir in Charakteristik 0 sind, ist $K \subseteq M''$ eine Galoiserweiterung. Wir können also davon ausgehen, dass eine Kette

$$K = L_0 \subseteq K(\zeta) = L_1 \subseteq L_2 \subseteq \ldots \subseteq L_k = M$$

vorliegt, wobei $K \subseteq M$ galoissch ist und wo die sukzessiven Körpererweiterungen $L_i \subseteq L_{i+1}$ einfache Radikalerweiterungen sind. Es sei $G = \mathrm{Gal}\,(M|K)$ und wir setzen

$$G_i \;=\; \mathrm{Gal}\,(M|L_i).$$

Dabei gelten nach Lemma 15.2 die natürlichen Inklusionen

$$G_k = \{\mathrm{id}\} \subseteq G_{k-1} \subseteq G_{k-2} \subseteq \ldots \subseteq G_1 \subseteq G_0 = G\,.$$

Da die Zwischenerweiterungen $L_i \subseteq L_{i+1}$ für $i \geq 1$ einfache Radikalerweiterungen und in L_1 die benötigten Einheitswurzeln vorhanden sind, folgt aus Satz 17.5, dass es sich um Galoiserweiterungen mit abelscher Galoisgruppe handelt. Aufgrund von Satz 16.4 sind daher die G_{i+1} Normalteiler in G_i und die Restklassengruppen G_i/G_{i+1} sind kommutativ. Die Erweiterung $K \subseteq K(\zeta) = L_1$ besitzt nach Aufgabe 19.11 ebenfalls eine abelsche Galoisgruppe. Daher liegt insgesamt eine Filtrierung vor, die G als auflösbar erweist. Da $K \subseteq L$ eine Galoiserweiterung ist, gilt wieder nach Satz 16.4 die Beziehung

$$\mathrm{Gal}\,(L|K) \;=\; G/\,\mathrm{Gal}\,(M|L),$$

so dass auch $\mathrm{Gal}\,(L|K)$ wegen Lemma 20.3 eine auflösbare Gruppe ist.

Sei nun vorausgesetzt, dass die Galoisgruppe $G = \mathrm{Gal}\,(L|K)$ auflösbar ist, und sei

$$\{\mathrm{Id}\} = G_k \subseteq G_{k-1} \subseteq G_{k-2} \subseteq \ldots \subseteq G_1 \subseteq G_0 = G$$

eine Filtrierung mit Untergruppen derart, dass jeweils $G_{i+1} \subseteq G_i$ ein Normalteiler ist mit abelscher Restklassengruppe G_i/G_{i+1}. Wir setzen $L_i = \mathrm{Fix}\,(G_i)$, so dass nach Lemma 15.2 und Satz 15.6 die Körperkette

$$K = L_0 \subseteq L_1 \subseteq \ldots \subseteq L_k = L$$

vorliegt. Dabei sind nach Korollar 15.7 die Körpererweiterungen $L_i \subseteq L$ galoissch, und ihre Galoisgruppen sind G_i gemäß Satz 16.1. Da die G_{i+1} Normalteiler in G_i sind, sind aufgrund von Satz 16.4 die Körpererweiterungen $L_i \subseteq L_{i+1}$ galoissch mit Galoisgruppe $\mathrm{Gal}\,(L_{i+1}|L_i) = G_i/G_{i+1}$. Diese sukzessiven Erweiterungen sind also Galoiserweiterungen mit abelscher Galoisgruppe. Es sei m der Exponent von G. Es sei $L \subseteq M$ ein m-ter Kreisteilungskörper, also ein Zerfällungskörper von $X^m - 1$ über L, und sei $\zeta \in M$ eine m-te primitive Einheitswurzel. Es ist somit $M = L(\zeta)$. Wir setzen $M_i = L_i(\zeta)$ (innerhalb von M) und haben dann die Körperkette

$$K \subseteq M_0 = K(\zeta) \subseteq M_1 \subseteq \ldots \subseteq M_k = M\,.$$

Hierbei gilt $M_{i+1} = M_i L_{i+1}$. Nach Satz 19.6 ist $M_i \subseteq M_{i+1}$ ebenfalls galoissch, und es gilt die Untergruppenbeziehung

$$\mathrm{Gal}\,(M_{i+1}|M_i) = \mathrm{Gal}\,(L_{i+1}|L_{i+1} \cap M_i) \subseteq \mathrm{Gal}\,(L_{i+1}|L_i)\,,$$

so dass diese Galoisgruppen auch abelsch sind. Da die m-te primitive Einheitswurzel ζ zu M_0 gehört, sind die Erweiterungen $M_i \subseteq M_{i+1}$ allesamt Kummererweiterungen und damit nach Korollar 17.4 auch Radikalerweiterungen. Da auch $K \subseteq M_0 = K(\zeta)$ eine (einfache) Radikalerweiterung ist, ist

insgesamt $K \subseteq M$ eine Radikalerweiterung, die L umfasst. Somit ist $K \subseteq L$ auflösbar. □

KOROLLAR 21.7. *Es sei K ein Körper der Charakteristik 0 und sei $F \in K[X]$ ein Polynom. Dann ist F genau dann auflösbar, wenn die Galoisgruppe $\mathrm{Gal}\,(Z(F)|K)$ des Zerfällungskörpers von F auflösbar ist.*

Beweis. Wegen Satz 15.6 ist $K \subseteq Z(F)$ eine Galoiserweiterung, so dass die Aussage direkt aus Satz 21.6 folgt. □

Ein wichtiges unmittelbares Korollar aus der vorstehenden Charakterisierung ist die Auflösbarkeit mit Radikalen von polynomialen Gleichungen vom Grad vier, wobei man dieses Ergebnis auch direkt über die (recht komplizierten, aber) expliziten Cardanoschen Lösungsformeln zum vierten Grad erhalten kann.

KOROLLAR 21.8. *Es sei K ein Körper der Charakteristik 0 und sei $F \in K[X]$ ein Polynom vom Grad ≤ 4. Dann ist F auflösbar. D.h. es gibt eine Radikalerweiterung $K \subseteq M$, so dass F über M in Linearfaktoren zerfällt.*

Beweis. Es sei L der Zerfällungskörper von F über K, der aufgrund der Voraussetzung über die Charakteristik nach Satz 15.6 eine Galoiserweiterung ist. Sei $G = \mathrm{Gal}\,(L|K)$. Über L besitzt F maximal $d = \mathrm{grad}\,(F)$ Nullstellen. Nach Lemma 13.1 ist G eine Untergruppe der Permutationsgruppe der Nullstellen, also ist jedenfalls $G \subseteq S_4$. Wegen Lemma 20.8 und Lemma 20.2 ist somit G eine auflösbare Gruppe. Aus Satz 21.6 folgt daher die Auflösbarkeit des Zerfällungskörpers über K. □

Das entscheidende Schlussfolgerung aus der obigen Charakterisierung ist aber, dass nicht alle Gleichungen auflösbar sind. Das ist Gegenstand der nächsten Vorlesung.