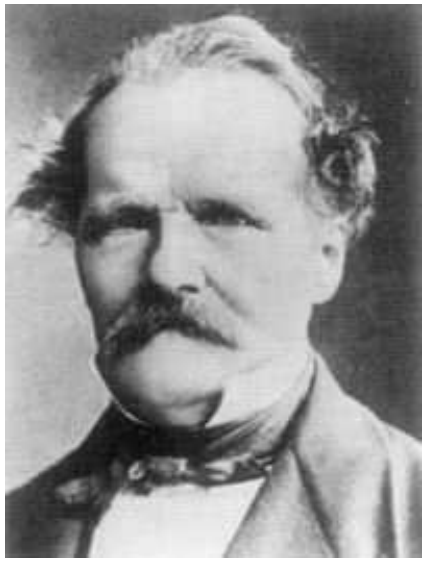
Prof. Dr. H. Brenner **Osnabrück WS 2018/2019**

Körper- und Galoistheorie

Vorlesung 18

Kummererweiterungen



Ernst Eduard Kummer (1810-1893)

Wir haben in der letzten Vorlesung gesehen, dass sich einige Eigenschaften einer Galoiserweiterung vereinfachen, wenn die Galoisgruppe abelsch ist. Beispielsweise ist dann jeder Zwischenkörper selbst galoissch über dem Grundkörper. Man spricht von *abelschen Galoiserweiterungen*.[1] Wichtige Beispiele solcher abelschen Körpererweiterungen sind Erweiterungen von endlichen Körpern und graduierte Körpererweiterungen, wenn hinreichend viele Einheitswurzeln im Grundkörper vorhanden sind.[2] Unter dieser Bedingung folgt umgekehrt, dass sich eine abelsche Erweiterung graduieren lässt. Dies ist der Inhalt der Kummertheorie.

Definition 18.1. Sei $m \in \mathbb{N}$ und sei K ein Körper, der eine m-te primitive Einheitswurzel enthält. Eine Galoiserweiterung $K \subseteq L$ heißt eine *Kummererweiterung* zum Exponenten m, wenn ihre Galoisgruppe abelsch und ihr Exponent ein Teiler von m ist.

[1] Es ist eine generelle Bezeichnungsphilosophie, dass ein Eigenschaftswort zu einer Galoiserweiterung sich auf die Galoisgruppe bezieht.

[2] Eine weitere wichtige Beispielsklasse sind die Kreisteilungskörper, siehe die beiden nächsten Vorlesungen.

SATZ 18.2. *Sei $m \in \mathbb{N}$ und sei K ein Körper, der eine m-te primitive Einheitswurzel enthält. Es sei $K \subseteq L$ eine endliche Körpererweiterung. Dann gelten folgende Aussagen.*

(1) *Wenn $L = \bigoplus_{d\in D} L_d$ eine D-graduierte Körpererweiterung ist, so ist $K \subseteq L$ eine Kummererweiterung zum Exponenten m.*
(2) *Sei $K \subseteq L$ eine Kummererweiterung zum Exponenten m mit Galoisgruppe G. Es sei $D = \operatorname{Char}(G, K)$ die Charaktergruppe von G. Zu $\delta \in D$ sei*[3]

$$L_\delta = \{x \in L | \, \varphi(x) = \delta(\varphi) \cdot x \text{ für alle } \varphi \in G\}.$$

Dann ist $L = \bigoplus_{\delta\in D} L_\delta$ eine D-graduierte Körpererweiterung.

Beweis. (1). Dies ist eine Neuformulierung von Satz 14.11. (2). Nach Satz Anhang 8.3 sind sämtliche Automorphismen $\varphi \in G = \operatorname{Gal}(L|K)$ diagonalisierbar. Da die Galoisgruppe abelsch ist, folgt aus Satz Anhang 8.4. die simultane Diagonalisierbarkeit aller Automorphismen $\varphi_1, \ldots, \varphi_n$ $(n = \#(G))$. Das heißt, dass man $L = \bigoplus_{i=1}^n L_i$ mit eindimensionalen K-Untervektorräumen L_i schreiben kann, die unter jedem $\varphi \in \operatorname{Gal}(L|K)$ auf sich abgebildet werden. Zu jedem L_i und jedem φ ist dabei $\varphi(x) = \zeta_{i,\varphi} \cdot x$ für jedes $x \in L_i$, das Element $\zeta_{i,\varphi}$ beschreibt also den Eigenwert von φ auf L_i. Die Zuordnung

$$\delta_i \colon G \longrightarrow K^\times, \, \varphi \longmapsto \zeta_{i,\varphi},$$

ist dabei ein Charakter. Es ist $L_i \subseteq L_{\delta_i}$, da ja L_i die zu δ_i gehörende Eigenraumbedingung erfüllt. Wegen

$$n = \operatorname{grad}_K L = \#(G) = \#(D)$$

ist $L_i = L_{\delta_i}$ und jeder Charakter δ tritt als ein δ_i auf. Also ist $L = \bigoplus_{\delta\in D} L_\delta$. Die Stufe zum konstanten Charakter ist K. Für $x_1 \in L_{\delta_1}$ und $x_2 \in L_{\delta_2}$ und $\varphi \in G$ ist

$$\begin{aligned} \varphi(x_1x_2) &= \varphi(x_1)\varphi(x_2) \\ &= \delta_1(\varphi)x_1\delta_2(\varphi)x_2 \\ &= \delta_1(\varphi)\delta_2(\varphi)x_1x_2 \\ &= (\delta_1 \cdot \delta_2)(\varphi)x_1x_2, \end{aligned}$$

also $x_1x_2 \in L_{\delta_1\cdot\delta_2}$, so dass in der Tat eine graduierte Körpererweiterung vorliegt. □

Ein Beispiel wie $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{-3}, \sqrt[3]{7}]$ zeigt, dass eine graduierte Körpererweiterung galoissch sein kann mit einer nichtkommutativen Galoisgruppe.

[3]Hier orientiert sich die Indizierung - entgegen der sonst üblichen additiven Schreibweise für eine graduierende Gruppe - an der multiplikativen Struktur von $\operatorname{Char}(G, K)$. Insbesondere ist L_1 die Stufe zum neutralen Element.

Korollar 18.3. *Sei $m \in \mathbb{N}$ und sei K ein Körper, der eine m-te primitive Einheitswurzel enthält. Es sei $K \subseteq L$ eine Kummererweiterung zum Exponenten m mit Galoisgruppe G, zugehöriger Charaktergruppe*

$$D = \operatorname{Char}(G, K)$$

und zugehöriger Graduierung

$$L = \bigoplus_{d \in D} L_d.$$

Es seien $H^\times$ die homogenen Elemente $\neq 0$ von L. Dann ist die natürliche Inklusion

$$H^\times \longrightarrow \left\{ a \in L^\times \mid a^m \in K \right\}$$

ein Gruppenisomorphismus.

Beweis. Die Charaktergruppe $D = \operatorname{Char}(G, K)$ besitzt wegen der Voraussetzung über die Einheitswurzeln nach Lemma 14.10 den gleichen Exponenten wie G. Für ein homogenes Element $x \in L_d$ gilt also insbesondere $x^m \in L_{dm} = L_0 = K$,[4] so dass die linke Menge eine Teilmenge der rechten ist. Die Multiplikation ist links und rechts gleich, so dass eine Untergruppe vorliegt. Zum Nachweis der Surjektivität sei $a \in L^\times$ mit $a^m \in K$ vorgegeben. Wir zeigen, dass ein solches Element einen Charakter der Galoisgruppe definiert. Zu $\varphi \in \operatorname{Gal}(L|K)$ ist

$$\left(\frac{\varphi(a)}{a}\right)^m = \frac{(\varphi(a))^m}{a^m} = \frac{\varphi(a^m)}{a^m} = \frac{a^m}{a^m} = 1.$$

Der Bruch $\delta_a(\varphi) = \frac{\varphi(a)}{a}$ ist also eine m-te Einheitswurzel und gehört somit zu $K^\times$. Für zwei Automorphismen $\varphi, \psi \in \operatorname{Gal}(L|K)$ ist dabei

$$\begin{aligned} \frac{(\varphi \circ \psi)(a)}{a} &= \frac{\varphi(\psi(a))}{a} \\ &= \frac{\varphi(a)}{a} \cdot \frac{\varphi(\psi(a))}{\varphi(a)} \\ &= \frac{\varphi(a)}{a} \cdot \varphi\left(\frac{\psi(a)}{a}\right) \\ &= \frac{\varphi(a)}{a} \cdot \frac{\psi(a)}{a}, \end{aligned}$$

so dass

$$\delta_a \colon \operatorname{Gal}(L|K) \longrightarrow K^\times,\ \varphi \longmapsto \frac{\varphi(a)}{a},$$

ein Charakter ist. Wegen $\varphi(a) = \frac{\varphi(a)}{a} a = \delta_a(\varphi) a$ ist $a \in L_{\delta_a}$, also homogen. □

Korollar 18.4. *Sei $m \in \mathbb{N}$ und sei K ein Körper, der eine m-te primitive Einheitswurzel enthält. Es sei $K \subseteq L$ eine Kummererweiterung zum Exponenten m. Dann ist $K \subseteq L$ eine Radikalerweiterung.*

[4] Hier verwenden wir wieder additive Schreibweise.

Beweis. Dies folgt direkt aus Satz 18.2 und aus Lemma 12.10 (5). □

Innerhalb der Radikalerweiterungen sind die Kummererweiterungen speziell, nämlich von der folgenden Gestalt.

Satz 18.5. *Sei $m \in \mathbb{N}$ und sei K ein Körper, der eine m-te primitive Einheitswurzel enthält. Es sei $K \subseteq L$ eine Körpererweiterung. Dann ist $K \subseteq L$ genau dann eine Kummererweiterung zum Exponenten m, wenn es eine Beschreibung*

$$L = K\left(\sqrt[m]{a_1}, \ldots, \sqrt[m]{a_r}\right)$$

mit $a_i \in K$ gibt.

Beweis. Aus Satz 18.2 und Lemma 12.10 (3) folgt, dass eine Kummererweiterung die angegebene Radikaldarstellung besitzt. Zum Beweis der Umkehrung sei $L = K(x_1, \ldots, x_r)$ mit $x_i^m = a_i \in K$. Wir müssen zeigen, dass diese Erweiterung galoissch mit abelscher Galoisgruppe ist. Es sei $\zeta \in K$ eine primitive m-te Einheitswurzel. Die Produkte $\zeta^\ell x_i$ erfüllen ebenfalls $\left(\zeta^\ell x_i\right)^m = a_i$. Da man die x_i als von 0 verschieden annehmen kann, und ζ primitiv ist, sind diese Produkte für jedes i untereinander verschieden. Dies bedeutet, dass die Polynome $X^m - a_1, \ldots, X^m - a_r$ über L in verschiedene Linearfaktoren zerfallen. Damit ist L der Zerfällungskörper dieser separablen Polynome, so dass nach Satz 16.6 eine Galoiserweiterung vorliegt. Sei $G = \mathrm{Gal}(L|K)$ die Galoisgruppe dieser Erweiterung. Für jedes $\varphi \in G$ und jedes i ist $\varphi(x_i)$ ebenfalls eine Lösung der Gleichung $X^m = a_i$ und daher ist $\varphi(x_i) = \zeta^\ell x_i$ mit einem gewissen (von φ und i abhängigen) ℓ. Für zwei Automorphismen $\varphi_1, \varphi_2 \in G$ ist daher

$$(\varphi_1 \circ \varphi_2)(x_i) = \varphi_1(\varphi_2(x_i)) = \varphi_1(\zeta^{\ell_2} x_i) = \zeta^{\ell_2}\varphi_1(x_i) = \zeta^{\ell_2}\zeta^{\ell_1} x_i = \zeta^{\ell_2+\ell_1} x_i.$$

Somit wirken die Automorphismen auf dem Erzeugendensystem kommutativ und daher ist $\varphi_1 \circ \varphi_2 = \varphi_2 \circ \varphi_1$. Damit ist die Galoisgruppe abelsch. Für jedes x_i ist ferner

$$\varphi^m(x_i) = \left(\zeta^\ell\right)^m x_i = x_i$$

mit einem gewissen ℓ. Also ist $\varphi^m = \mathrm{Id}$, so dass m ein Vielfaches des Exponenten ist. □

Beispiel 18.6. Der achte Kreisteilungskörper über $\mathbb{Q}$, also die (siehe Beipiel 9.15) (mehrfach) graduierte Körpererweiterung

$$\mathbb{Q} \subseteq L = K_8 = \mathbb{Q}[\mathrm{i}, \sqrt{2}] = \mathbb{Q}[X]/(X^4 + 1)$$

ist eine Kummererweiterung zum Exponenten 2 mit Galoisgruppe $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$. Die gemäß Satz 18.2 zugehörige $\mathbb{Z}/(2) \times \mathbb{Z}/(2)$-Graduierung ist

$$\mathbb{Q} \oplus \mathbb{Q}\mathrm{i} \oplus \mathbb{Q}\sqrt{2} \oplus \mathbb{Q}\mathrm{i}\sqrt{2}\,.$$

Nach Korollar 18.3 gilt $H^\times = \{a \in L^\times | \, a^2 \in \mathbb{Q}\}$, d.h. die Menge der rationalen Quadratwurzeln von L sind einfach beschreibbar. Es gibt aber auch noch weitere Wurzeln aus rationalen Zahlen in L, beispielsweise die achte Einheitswurzel ζ_8, die eine vierte Wurzel von -1 ist.

Das Lemma von Gauss und das Eisensteinkriterium

In der nächsten Vorlesung werden wir uns mit Kreisteilungskörpern beschäftigen. Dazu brauchen wir einige wichtige Irreduzibilitätskriterien für Polynome aus $\mathbb{Q}[X]$.

Die folgende Aussage heißt *Lemma von Gauß*.

LEMMA 18.7. *Es sei $f \in \mathbb{Z}[X]$ ein nichtkonstantes Polynom derart, dass in $\mathbb{Z}[X]$ nur Faktorzerlegungen $f = gh$ mit $g \in \mathbb{Z}$ oder $h \in \mathbb{Z}$ möglich sind. Dann ist f irreduzibel in $\mathbb{Q}[X]$.*

Beweis. Nehmen wir an, es gebe eine nicht-triviale Faktorzerlegung $f = gh$ mit nicht-konstanten Polynomen $g, h \in \mathbb{Q}[X]$. Sowohl in g als auch in h kommen nur endlich viele Nenner aus $\mathbb{Z}$ vor, so dass man mit einem gemeinsamen Hauptnenner $r \in \mathbb{Z}$ multiplizieren kann und somit eine Darstellung $rf = \tilde{g}\tilde{h}$ mit $\tilde{g}, \tilde{h} \in \mathbb{Z}[X]$ erhält. Dabei haben sich die Grade der beteiligten Polynome nicht geändert. Es sei $r = p_1 \cdots p_n$ die Primfaktorzerlegung von r. Nach Aufgabe 3.19 ist p_1 auch im Polynomring $\mathbb{Z}[X]$ prim. Da es das Produkt $\tilde{g}\tilde{h}$ teilt, muss es einen der Faktoren teilen, sagen wir $\tilde{h}$. Dann kann man mit p_1 kürzen und erhält eine Gleichung der Form

$$r'f = \tilde{g}\tilde{h}'.$$

Dabei ändern sich wieder die Grade nicht. So kann man sukzessive alle Primfaktoren wegkürzen und erhält schließlich eine Zerlegung

$$f = g'h'$$

mit nicht konstanten Polynomen $h', g' \in \mathbb{Z}[X]$ im Widerspruch zur Voraussetzung. □

LEMMA 18.8. *Sei R ein Integritätsbereich und sei $F = \sum_{i=0}^{n} c_i X^i \in R[X]$ ein Polynom. Es sei $p \in R$ ein Primelement mit der Eigenschaft, dass p den Leitkoeffizienten c_n nicht teilt, alle anderen Koeffizienten teilt, aber dass p^2 nicht den konstanten Koeffizienten c_0 teilt. Dann besitzt F keine Zerlegung $F = GH$ mit nicht-konstanten Polynomen $G, H \in R[X]$.*

Beweis. Sei angenommen, dass es eine Zerlegung $F = GH$ mit nicht-konstanten Polynomen $G, H \in R[X]$ gebe, und sei $G = \sum_{i=0}^{k} a_i X^i$ und $H = \sum_{j=0}^{m} b_j X^j$. Dann ist $c_0 = a_0 b_0$ und dies ist ein Vielfaches von p, aber nicht von p^2. Da p prim ist, teilt es einen der Faktoren, sagen wir a_0, aber nicht den anderen. Es ist nicht jeder Koeffizient von G ein Vielfaches von p, da sonst G und damit auch F ein Vielfaches von p wäre, was aber aufgrund der Bedingung an den Leitkoeffizienten ausgeschlossen ist. Es sei r der kleinste Index derart, dass a_r kein Vielfaches von p ist. Es ist $r \leq \operatorname{grad}(G) < \operatorname{grad}(F)$, da H nicht konstant ist. Wir betrachten den Koeffizienten c_r, für den

$$c_r = a_0 b_r + a_1 b_{r-1} + \cdots + a_{r-1} b_1 + a_r b_0$$

gilt. Hierbei sind c_r und alle Summanden $a_i b_{r-i}$, $i = 0, \ldots, r-1$, Vielfache von p. Daher muss auch der letzte Summand $a_r b_0$ ein Vielfaches von p sein. Dies ist aber ein Widerspruch, da $p \nmid a_r$ und $p \nmid b_0$. □

Das folgende Kriterium für die Irreduzibilität von Polynomen heißt *Eisenstein-Kriterium*.

SATZ 18.9. *Es sei $F = \sum_{i=0}^{n} c_i X^i \in \mathbb{Z}[X]$ ein Polynom. Es sei $p \in \mathbb{Z}$ eine Primzahl mit der Eigenschaft, dass p den Leitkoeffizienten c_n nicht teilt, aber alle anderen Koeffizienten teilt, aber dass p^2 nicht den konstanten Koeffizienten c_0 teilt. Dann ist F irreduzibel in $\mathbb{Q}[X]$.*

Beweis. Dies folgt aus Lemma 18.8 und Lemma 18.7. □

Abbildungsverzeichnis