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

Körper- und Galoistheorie

Vorlesung 12

Wir interessieren uns für die Frage, wann eine endliche Körpererweiterung $K \subseteq L$ einfach ist, also in der Form $L = K(x)$ mit einem Element $x \in L$ geschrieben werden kann. Antwort gibt der *Satz vom primitiven Element* (d.h. erzeugenden Element), der besagt, dass dies unter der recht schwachen Voraussetzung der Separabilität der Fall ist.

Separable Körpererweiterungen

Definition 12.1. Es sei K ein Körper. Ein Polynom $P \in K[X]$ heißt *separabel*, wenn es über keinem Erweiterungskörper $K \subseteq L$ mehrfache Nullstellen besitzt.

Lemma 12.2. *Es sei K ein Körper und sei $P \in K[X]$ ein Polynom. Dann sind die folgenden Aussagen äquivalent.*

(1) *P ist separabel.*
(2) *Es gibt eine Körpererweiterung $K \subseteq L$ derart, dass P über L in einfache Linearfaktoren zerfällt.*
(3) *P und die Ableitung P' sind teilerfremd.*
(4) *P und die Ableitung P' erzeugen das Einheitsideal.*

Beweis. (1) $\Rightarrow$ (2). Dies folgt aus Lemma 11.1. (2) $\Rightarrow$ (3). Nehmen wir an, dass P und P' einen gemeinsamen nichttrivialen Teiler in $K[X]$ besitzen. Dies ist dann auch in $L[X]$ der Fall. Dies bedeutet wiederum, dass ein Linearfaktor von P auch ein Teiler von P' ist. Daher besitzen P und P' eine gemeinsame Nullstelle und somit besitzt P eine mehrfache Nullstelle im Widerspruch zur Voraussetzung. (3) $\Rightarrow$ (4). Dies folgt aus Lemma 3.16. (4) $\Rightarrow$ (1). Sei $K \subseteq L$ eine Körpererweiterung, so dass $P \in L[X]$ in Linearfaktoren zerfällt. Nach Voraussetzung kann man 1 in $K[X]$ als Linearkombination von P und P' darstellen. Diese Eigenschaft überträgt sich direkt auf $L[X]$. Wenn P in L eine mehrfache Nullstelle hätte, so wäre diese Nullstelle auch eine Nullstelle der Ableitung. Das kann aber wegen der Darstellbarkeit der 1 nicht sein. □

Definition 12.3. Eine endliche Körpererweiterung $K \subseteq L$ heißt *separabel*, wenn für jedes Element $x \in L$ das Minimalpolynom separabel ist.

Lemma 12.4. *Es sei $K \subseteq L$ eine endliche separable Körpererweiterung und M, $K \subseteq M \subseteq L$, ein Zwischenkörper. Dann ist auch $M \subseteq L$ eine separable Körpererweiterung.*

Beweis. Siehe Aufgabe 12.5. □

Unser erstes wichtiges Ziel ist es, zu zeigen, dass eine endliche Körpererweiterung bereits dann separabel ist, wenn die Minimalpolynome zu einem Erzeugendensystem separabel sind.

LEMMA 12.5. *Es sei $K \subseteq L = K[x] = K(x)$ eine einfache Körpererweiterung vom Grad $d = \operatorname{grad}_K L$. Es sei $K \subseteq M$ eine Körpererweiterung, unter der das Minimalpolynom F von x in Linearfaktoren zerfällt. Dann ist F genau dann ein separables Polynom, wenn es d verschiedene K-Einbettungen von L in M gibt.*

Beweis. Es sei also $K \subseteq L = K[x] = K[X]/(F)$ vom Grad d mit dem Minimalpolynom F gegeben. Dieses Polynom F ist genau dann separabel, wenn es in M genau d Nullstellen besitzt. Diese Nullstellen stehen gemäß Satz 6.4 in Bijektion zu den K-Algebra-Homomorphismen von $L = K[X]/(F)$ nach M. □

LEMMA 12.6. *Es sei $K \subseteq L = K[x_1, \ldots, x_n]$ eine endliche Körpererweiterung vom Grad $d = \operatorname{grad}_K L$ mit der Eigenschaft, dass die Minimalpolynome $F_i \in K[X]$ zu den x_i separabel sind. Es sei $K \subseteq M$ eine Körpererweiterung, unter der die F_i in Linearfaktoren zerfallen. Dann gibt es d verschiedene K-Einbettungen von L in M.*

Beweis. Wir führen Induktion über n, bei $n = 0$ ist der Grad der Körpererweiterung gleich 1 und es gibt auch nur die K-Einbettung $K \subseteq M$. Sei die Aussage für n bewiesen. Wir betrachten die Körperkette

$$K \subseteq K' = K[x_1, \ldots, x_n] \subseteq K'[x_{n+1}] = L\,.$$

Wir wissen also, dass es $\operatorname{grad}_K K'$ verschiedene K-Einbettungen von K' nach M gibt. Aufgrund der Gradformel genügt es zu zeigen, dass es für $K' \subseteq K'[x_{n+1}] = L$ so viele K'-Einbettungen von L in M gibt, wie es der Körpergrad $\operatorname{grad}_{K'} L$ vorgibt. Es genügt also, den Fall $n = 1$ zu beweisen, und dieser folgt aus Lemma 12.5. □

SATZ 12.7. *Es sei $K \subseteq L = K[x_1, \ldots, x_n]$ eine endliche Körpererweiterung. Es sei vorausgesetzt, dass die Minimalpolynome F_i der x_i separabel sind. Dann ist die Erweiterung $K \subseteq L$ separabel.*

Beweis. Es sei $x \in L$ mit Minimalpolynom $F \in K[X]$. Wir betrachten den zugehörigen Zwischenkörper $K \subseteq K[x] \cong K[X]/(F) \subseteq L$, wobei die Grade mit $d_1 = \operatorname{grad}_K K[x]$, $d_2 = \operatorname{grad}_{K[x]} L$ und mit $d = d_1 d_2 = \operatorname{grad}_K L$ bezeichnet seien. Es sei $L \subseteq M$ ein Körper, über dem F und die F_i in Linearfaktoren zerfallen. Nach Lemma 12.6 gibt es d K-Algebra-Homomorphismen von L nach M. Wenn die Anzahl der Homomorphismen von $K[x]$ nach M kleiner als d_1 wäre, so würde es mehr als d_2 Homomorphismen $L \to M$ geben, deren Einschränkungen auf $K[x]$ übereinstimmen würden. Nach Lemma 12.4 ist $K[x] \subseteq L$ eine separable Körperweiterung vom Grad d_2 und daher gibt es nach Lemma 12.5 genau d_2 Homomorphismen von L nach M über $K[x]$ ist,

so dass das nicht sein kann. Also gibt es d_1 Algebra-Homomorphismen von $K[x] \cong K[X]/(F)$ nach M und somit ist F, wiederum nach Lemma 12.5, ein separables Polynom. □

Der Satz vom primitiven Element

LEMMA 12.8. *Es sei $K \subseteq L = K(x)$ eine endliche einfache Körpererweiterung und $K \subseteq M \subseteq L$ ein Zwischenkörper. Es sei $G = \sum_{j=0}^{k} b_j X^j \in M[X]$ das Minimalpolynom von x über M. Dann ist $M = K(b_0, \ldots, b_k)$.*

Beweis. Wir gehen von der Inklusion $K' = K(b_0, \ldots, b_k) \subseteq M$ aus. Die Körpererweiterung $K' \subseteq L$ ist ebenfalls einfach mit dem Erzeuger x, und $G \in K'[X]$ ist irreduzibel, da es ja irreduzibel in $M[X]$ ist. Somit ist G nach Lemma 7.12 auch das Minimalpolynom von x über K'. Daher ist $L = M[X]/(G)$ und $L = K'[X]/(G)$ und insbesondere

$$\operatorname{grad}_M L \;=\; \operatorname{Grad}(G) \;=\; \operatorname{grad}_{K'} L.$$

Nach der Gradformel folgt $K' = M$. □

SATZ 12.9. *Sei $K \subseteq L$ eine endliche Körpererweiterung. Dann ist $K \subseteq L$ genau dann eine einfache Körpererweiterung, wenn es nur endlich viele Zwischenkörper $K \subseteq M \subseteq L$ gibt.*

Beweis. Wenn K ein endlicher Körper ist, so ist auch L endlich und die Voraussetzung über die endlich vielen Zwischenkörper ist automatisch erfüllt. In diesem Fall ist aber auch nach Satz 10.5 die Körpererweiterung einfach. Wir können also annehmen, dass K unendlich ist. Sei zunächst vorausgesetzt, dass es in $K \subseteq L$ nur endlich viele Zwischenkörper gibt. Sei $\operatorname{grad}_K L = n$. Jeder von L verschiedene Zwischenkörper M_i ist ein maximal $(n-1)$-dimensionaler K-Untervektorraum von L und daher gibt es eine von 0 verschiedene K-lineare Abbildung

$$\varphi_i : L \longrightarrow K$$

mit $\varphi_i(M_i) = 0$. Zu φ_i gehört ein lineares Polynom P_i (in n Variablen)[1] mit der entsprechenden Eigenschaft. Das Polynom $P = \prod_{i=1}^{k} P_i$ ist dann auf der Vereinigung aller Zwischenkörper $M_i \neq L$ gleich 0. Da K unendlich ist, gibt es aber nach Aufgabe 12.11 auch Elemente $a = (a_1, \ldots, a_n) \in L$ mit $P(a) \neq 0$. Der von einem solchen Element a über K erzeugte Körper muss gleich L sein, da er nach Konstruktion in keinem anderen Zwischenkörper liegt. Sei nun $L = K(x) = K[x] = K[X]/(F)$ eine einfache Körpererweiterung mit dem Minimalpolynom $F \in K[X]$. Für jeden Zwischenkörper M, $K \subseteq M \subseteq L$, ist $L = M(x)$ und das Minimalpolynom G von x über M ist in $M[X]$ und insbesondere in $L[X]$ ein Teiler von F. Nach Lemma 12.8 besteht die Beziehung $M = K(b_0, \ldots, b_k)$, wobei die b_j die Koeffizienten von G sind.

[1] Man fixiert hierzu eine K-Basis von L, die zugehörige Dualbasis entspricht dann den n Variablen. Die folgende Tupelschreibweise bezieht sich ebenfalls auf die Basis.

Da F nur endlich viele (normierte) Teiler besitzt, gibt es nur endlich viele Zwischenkörper. □

KOROLLAR 12.10. *Es sei $K \subseteq L$ eine endliche einfache Körpererweiterung und $K \subseteq M \subseteq L$ ein Zwischenkörper. Dann ist auch $K \subseteq M$ eine einfache Körpererweiterung.*

Beweis. Dies folgt unmittelbar aus Satz 12.9, da ja $K \subseteq M$ unter der Voraussetzung auch nur endlich viele Zwischenkörper besitzt. □

Der folgende Satz heißt *Satz vom primitiven Element.*

SATZ 12.11. *Sei $K \subseteq L$ eine separable endliche Körpererweiterung. Dann wird L von einem Element erzeugt, d.h. es gibt ein $f \in L$ mit*

$$L = K(f) \cong K[X]/(P)$$

mit einem irreduziblen (Minimal-)Polynom $P \in K[X]$.

Beweis. Bei K endlich folgt die Aussage sofort aus Satz 10.5, wir können also K als unendlich annehmen. Es sei $K \subseteq L = K[x_1, \ldots, x_n]$. Es genügt zu zeigen, dass man sukzessive zwei Erzeuger davon durch einen Erzeuger ersetzen kann. Dabei ist $K \subseteq K[x_1, x_2]$ ebenfalls separabel. Sei also $L = K[x, y]$ gegeben und $n = \operatorname{grad}_K L$. Es sei $K \subseteq M$ eine Körpererweiterung, bei der die Minimalpolynome von x und von y in Linearfaktoren zerfallen. Es gibt gemäß Lemma 12.6 n K-Einbettungen

$$\sigma_1, \ldots, \sigma_n : L \longrightarrow M.$$

Wir betrachten das Polynom

$$P = \prod_{i \neq j} ((\sigma_i(y) - \sigma_j(y))X + \sigma_i(x) - \sigma_j(x)) \,,$$

das zu $M[X]$ gehört. Dies ist nicht das Nullpolynom, da keiner der Linearfaktoren gleich 0 ist. Daher besitzt P nur endlich viele Nullstellen und somit gibt es, da K unendlich ist, ein $c \in K$ mit $P(c) \neq 0$. Die Elemente $\sigma_i(x + cy) = \sigma_i(x) + c\sigma_i(y)$ sind alle verschieden. Aus $\sigma_i(x) + c\sigma_i(y) = \sigma_j(x) + c\sigma_j(y)$ für $i \neq j$ folgt nämlich $(\sigma_i(y) - \sigma_j(y))c + \sigma_i(x) - \sigma_j(x) = 0$, und c wäre doch eine Nullstelle. Es gibt also n verschiedene Einbettungen von $K(x + cy)$ nach M und insbesondere ist $\operatorname{grad}_K K[x + cy] \geq n$, also ist $K(x + cy) = L$. □