Prof. Dr. H. Brenner **Osnabrück SS 2009**

Einführung in die Algebra

Vorlesung 23

Die Gradformel

Satz 1. *Seien $K \subseteq L$ und $L \subseteq M$ endliche Körperweiterungen. Dann ist auch $K \subseteq M$ eine endliche Körpererweiterung und es gilt*

$$\operatorname{grad}_K M = \operatorname{grad}_K L \cdot \operatorname{grad}_L M .$$

Beweis. Wir setzen $\operatorname{grad}_K L = n$ und $\operatorname{grad}_L M = m$. Es sei $x_1, \ldots, x_n \in L$ eine K-Basis von L und $y_1, \ldots, y_m \in M$ eine L-Basis von M. Wir behaupten, dass die Produkte

$$x_i y_j,\ 1 \leq i \leq n,\ 1 \leq j \leq m,$$

eine K-Basis von M bilden. Wir zeigen zuerst, dass diese Produkte den Vektorraum M über K aufspannen. Sei dazu $z \in M$. Wir schreiben

$$z = b_1 y_1 + \ldots + b_m y_m \text{ mit Koeffizienten } b_j \in L.$$

Wir können jedes b_j als $b_j = a_{1j}x_1 + \ldots + a_{nj}x_n$ mit Koeffizienten $a_{ij} \in K$ ausdrücken. Das ergibt

$$\begin{aligned} z &= b_1 y_1 + \ldots + b_m y_m \\ &= a_{11}x_1 + \ldots + a_{n1}x_n)y_1 + \ldots + (a_{1m}x_1 + \ldots + a_{nm}x_n)y_m \\ &= \sum_{1 \leq i \leq n,\, 1 \leq j \leq m} a_{ij} x_i y_j. \end{aligned}$$

Daher ist z eine K-Linearkombination der Produkte $x_i y_j$. Um zu zeigen, dass diese Produkte linear unabhängig sind, sei

$$0 = \sum_{1 \leq i \leq n,\, 1 \leq j \leq m} c_{ij} x_i y_j$$

angenommen mit $c_{ij} \in K$. Wir schreiben dies als $0 = \sum_{j=1}^{m} (\sum_{i=1}^{n} c_{ij} x_i) y_j$. Da die y_j linear unabhängig über L sind und die Koeffizienten der y_j zu L gehören folgt, dass $\sum_{i=1}^{n} c_{ij} x_i = 0$ ist für jedes j. Da die x_i linear unabhängig über K sind und $c_{ij} \in K$ ist folgt, dass $c_{ij} = 0$ ist für alle i, j. □

Zerfällungskörper

Lemma 2. *Sei K ein Körper und F ein Polynom aus $K[X]$. Dann gibt es einen Erweiterungskörper $K \subseteq L$ derart, dass F über L in Linearfaktoren zerfällt.*

Beweis. Sei $F = P_1 \cdots P_r$ die Zerlegung in Primpolynome in $K[X]$, und sei P_1 nicht linear. Dann ist

$$K \longrightarrow K[Y]/(P_1) =: K'$$

eine Körpererweiterung von K nach Satz 18.5 Wegen $P_1(Y) = 0$ in K' ist die Restklasse y von Y in K' eine Nullstelle von P_1. Daher gilt in $K'[X]$ die Faktorisierung

$$P_1 = (X - y)\tilde{P}\,,$$

wobei $\tilde{P}$ kleineren Grad als P_1 hat. Das Polynom F hat also über K' mindestens einen Linearfaktor mehr als über K. Induktive Anwendung von dieser Konstruktion liefert eine Kette von Erweiterungen $K \subset K' \subset K'' \ldots$, die stationär wird, sobald F in Linearfaktoren zerfällt. □

Definition 3. Es sei K ein Körper, $F \in K[X]$ ein Polynom und $K \subseteq L$ eine Körpererweiterung, über der F in Linearfaktoren zerfällt. Es seien $a_1, \ldots, a_n \in L$ die Nullstellen von F. Dann nennt man

$$K[a_1, \ldots, a_n] \subseteq L$$

einen *Zerfällungskörper* von F.

Es handelt sich hierbei wirklich um einen Körper, wie wir gleich sehen werden. Häufig beschränkt man sich auf Polynome vom Grad ≥ 1, bei konstanten Polynomen sehen wir einfach K selbst als Zerfällungskörper an. Über dem Zerfällungskörper zerfällt das gegebene Polynom in Linearfaktoren, da er ja nach Definition alle Nullstellen enthält, mit denen alle beteiligten Linearfaktoren formuliert werden können.

Lemma 4. *Sei K ein Körper, $F \in K[X]$ ein Polynom und L ein Zerfällungskörper für F. Es sei $K \subseteq K' \subseteq L$ ein Zwischenkörper. Dann ist auch L ein Zerfällungskörper des Polynoms $F \in K'[X]$.*

Beweis. Das ist trivial. □

Lemma 5. *Sei K ein Körper, $F \in K[X]$ ein Polynom und L ein Zerfällungskörper für F. Dann ist $K \subseteq L$ eine endliche Körpererweiterung.*

Beweis. Es sei $L = K[a_1, \ldots, a_n]$, wobei $a_i \in L$ die Nullstellen von F seien und F über L in Linearfaktoren zerfällt. Es liegt die Kette von K-Algebren

$$K \subseteq K[a_1] \subseteq K[a_1, a_2] \subseteq \cdots \subseteq K[a_1, \ldots, a_n] = L$$

vor. Dabei ist sukzessive a_i algebraisch über $K[a_1, \ldots, a_{i-1}]$, da ja a_i eine Nullstelle von $F \in K[X]$ ist. Daher sind die Inklusionen nach Satz 22.2 endliche Körpererweiterungen und nach Satz 23.1 ist dann die Gesamtkörpererweiterung ebenfalls endlich. □

Satz 6. *Es sei K ein Körper und sei $F \in K[X]$ ein Polynom. Es seien $K \subseteq L_1$ und $K \subseteq L_2$ zwei Zerfällungskörper von F. Dann gibt es einen K-Algebra-Isomorphismus*

$$\varphi : L_1 \longrightarrow L_2.$$

Insbesondere gibt es bis auf Isomorphie nur einen Zerfällungskörper zu einem Polynom.

Beweis. Wir beweisen die Aussage durch Induktion über den Grad $\operatorname{grad}_K L_1$. Wenn der Grad eins ist, so ist $K = L_1$ und das Polynom F zerfällt bereits über K in Linearfaktoren. Dann gehören alle Nullstellen von F in einem beliebigen Erweiterungskörper $K \subseteq M$ zu K selbst. Also ist auch $L_2 = K$. Es sei nun $\operatorname{grad}_K L_1 \geq 2$ und die Aussage sei für kleinere Grade bewiesen. Dann zerfällt F über K nicht in Linearfaktoren. Daher gibt es einen irreduziblen Faktor P von F mit $\operatorname{grad}(P) \geq 2$ und $K' = K[X]/(P)$ ist nach Satz 18.5 und nach Proposition 21.3 eine Körpererweiterung von K vom Grad ≥ 2. Da P als Faktor von F ebenfalls über L_1 und über L_2 in Linearfaktoren zerfällt, gibt es Ringhomomorphismen $K' \to L_1$ und $K' \to L_2$. Diese sind injektiv, so dass K' sowohl von L_1 als auch von L_2 ein Unterkörper ist. Nach Lemma 23.4 sind dann L_1 und L_2 Zerfällungskörper von $F \in K'[X]$. Nach Satz 23.1 ist $\operatorname{grad}_{K'} L_1 < \operatorname{grad}_K L_1$, so dass wir auf K', L_1, L_2 die Induktionsvoraussetzung anwenden können. Es gibt also einen K'-Algebra-Isomorphismus

$$\varphi : L_1 \longrightarrow L_2.$$

Dieser ist erst recht ein K-Algebra-Isomorphismus. □

Konstruktion endlicher Körper

Endliche Körper mit der Anzahl p^n konstruiert man, indem man ein in $(\mathbb{Z}/(p))[X]$ irreduzibles Polynom vom Grad n findet. Ob ein gegebenes Polynom irreduzibel ist, lässt sich dabei grundsätzlich in endlich vielen Schritten entscheiden, da es ja zu jedem kleineren Grad überhaupt nur endlich viele Polynome gibt, die als Teiler in Frage kommen können. Zur Konstruktion von einigen kleinen endlichen Körpern siehe die Aufgaben Aufgabe 19.12 und Aufgabe 23.8. Generell kann man einen Körper mit $q = p^n$ Elementen als Zerfällungskörper des Polynoms $X^q - X$ erhalten.

Lemma 7. *Sei K ein Körper der Charakteristik p, sei $q = p^e$, $e \geq 1$. Es sei*

$$M = \left\{x \in K : x^q = x\right\}.$$

Dann ist M ein Unterkörper von K.

Beweis. Zunächst gilt für jedes Element $x \in \mathbb{Z}/(p) \subseteq K$, dass

$$x^{p^e} = (x^p)^{p^{e-1}} = x^{p^{e-1}} = \ldots = x$$

ist, wobei wir wiederholt den kleinen Fermat (Satz 14.14) benutzt haben. Insbesondere ist also $0, 1, -1 \in M$. Es ist $z^q = F^e(z)$ und der Frobenius

$$F : K \longrightarrow K,\, x \longmapsto x^p,$$

ist ein Ringhomomorphismus. Daher ist für $x, y \in M$ einerseits

$$(x+y)^q = F^e(x+y) = F^e(x) + F^e(y) = x^q + y^q = x + y$$

und andererseits

$$(xy)^q = x^q y^q = xy\,.$$

Ferner gilt für $x \in M$, $x \neq 0$, die Gleichheit

$$(x^{-1})^q = (x^q)^{-1} = x^{-1}\,,$$

so dass auch das Inverse zu M gehört und in der Tat ein Körper vorliegt. □

Im Beweis der nächsten Aussage werden wir die Technik des *formalen Ableitens* verwenden. Ableiten ist eigentlich eine analytische Technik, und bekanntlich ist die Ableitung eines Monoms X^m gleich mX^{m-1}, und die Ableitung eines Polynoms ergibt sich durch lineare Fortsetzung dieser Regel. Da der Exponent der Variablen zum Vorfaktor wird, und da man jede ganze Zahl in jedem Körper eindeutig interpretieren kann, machen solche Ableitungen auch rein algebraisch für jeden Grundkörper Sinn. Wir definieren daher.

Definition 8. Sei K ein Körper und sei $K[X]$ der Polynomring über K. Zu einem Polynom

$$F = \sum_{i=0}^{n} a_i X^i \in K[X]$$

heißt das Polynom

$$F' = na_n X^{n-1} + (n-1)a_{n-1}X^{n-2} + \ldots + 3a_3X^2 + 2a_2X + a_1$$

die *formale Ableitung* von F.

Man beachte, dass, insbesondere bei positiver Charakteristik, das algebraische Ableiten einige überraschende Eigenschaften haben kann. In positiver Charakteristik p ist bspw.

$$(X^p)' = pX^{p-1} = 0.$$

Für einige grundlegenden Eigenschaften des Ableitens siehe die Aufgaben. Wichtig ist für uns, dass man mit der formalen Ableitung testen kann, ob die Nullstellen eines Polynoms einfach oder mehrfach sind (eine Nullstelle a heißt *mehrfach*, wenn das zugehörige lineare Polynom $X - a$ das Polynom mehrfach teilt, d.h. es in der Primfaktorzerlegung mit einem Exponenten ≥ 2 vorkommt).

LEMMA 9. *Sei K ein Körper der Charakteristik p, sei $q = p^e$, $e \geq 1$. Das Polynom $X^q - X$ zerfalle über K in Linearfaktoren. Dann ist*

$$M = \{x \in K : x^q = x\}$$

ein Unterkörper von K mit q Elementen.

Beweis. Nach Lemma 23.7 ist M ein Unterkörper von K, und nach Korollar 18.10 besitzt er höchstens q Elemente. Es ist also zu zeigen, dass $F = X^q - X$ keine mehrfache Nullstellen hat. Dies folgt aber aus $F' = -1$ und Aufgabe 23.14. □

SATZ 10. *Sei p eine Primzahl und $e \in \mathbb{N}_+$. Dann gibt es bis auf Isomorphie genau einen Körper mit $q = p^e$ Elementen.*

Beweis. Existenz. Wir wenden das Lemma 23.2 auf den Grundkörper $\mathbb{Z}/(p)$ und das Polynom $X^q - X$ an und erhalten einen Körper L der Charakteristik p, über dem $X^q - X$ in Linearfaktoren zerfällt. Nach Lemma 23.9 gibt es dann einen Unterkörper M von L, der aus genau q Elementen besteht.

Eindeutigkeit. Wir zeigen, dass ein Körper mit q Elementen der Zerfällungskörper des Polynoms $X^q - X$ sein muss, so dass er aufgrund dieser Eigenschaft nach Satz 23.6 eindeutig bestimmt ist. Sei also L ein Körper mit q Elementen, der dann $\mathbb{Z}/(p)$ als Primkörper enthält. Da $L^\times$ genau $q-1$ Elemente besitzt, gilt nach Satz 7.4 die Gleichung $x^{q-1} = 1$ für jedes $x \in L^\times$ und damit auch $x^q = x$ für jedes $x \in L$. Dieses Polynom vom Grad q hat also in L genau q verschiedene Nullstellen, so dass es also über L zerfällt. Zugleich ist der von allen Nullstellenen erzeugte Unterkörper gleich L, so dass L der Zerfällungskörper ist. □

NOTATION 11. Sei p eine Primzahl und $e \in \mathbb{N}_+$. Der aufgrund von Satz 23.10 bis auf Isomorphie eindeutig bestimmte endliche Körper mit $q = p^e$ Elementen wird mit

$$\mathbb{F}_q$$

bezeichnet.

Für $q = p$ ist $\mathbb{F}_p = \mathbb{Z}/(p)$. Dagegen sind für $q = p^e$, $e \geq 2$, die Ringe $\mathbb{F}_q$ und $\mathbb{Z}/(q)$ verschieden, obwohl beide Ringe q Elemente besitzen. Dies liegt einfach daran, dass $\mathbb{F}_q$ ein Körper ist, $\mathbb{Z}/(q)$ aber nicht.