Prof. Dr. H. Brenner **Osnabrück SS 2015**

Elemente der Algebra

Vorlesung 24

Quadratische Körpererweiterungen

Die aller einfachste Körpererweiterung ist die *identische Körpererweiterung* $K = K$, die den Grad 1 besitzt. Die nächst einfachsten sind die vom Grad zwei.

DEFINITION 24.1. Eine endliche Körpererweiterung $K \subseteq L$ vom Grad zwei heißt eine *quadratische Körpererweiterung*.

Beispiele sind $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{p}]$, wobei p eine Primzahl ist (oder sonst eine rationale Zahl ohne rationale Quadratwurzel) oder $K = K[X]/(P)$ zu einem irreduziblen quadratischen Polynom $P = X^2 + aX + b$.

LEMMA 24.2. *Es sei K ein Körper mit einer Charakteristik $\neq 2$ und es sei $K \subset L$ eine quadratische Körpererweiterung. Dann gibt es ein $x \in L$, $x \notin K$ und $x^2 \in K$.*

Beweis. Nach Voraussetzung ist L ein zweidimensionaler Vektorraum über K, und darin ist $K = K1$ ein eindimensionaler Untervektorraum. Nach dem Basisergänzungssatz gibt es ein Element $y \in L$ derart, dass 1 und y eine K-Basis von L bilden. Wir können

$$y^2 = a + by$$

schreiben, bzw. (da 2 eine Einheit ist),

$$0 = y^2 - by - a = \left(y - \frac{b}{2}\right)^2 - \frac{b^2}{4} - a.$$

Mit $x = y - \frac{b}{2}$ gilt also $x^2 = \frac{b^2}{4} + a \in K$ und 1 und x bilden ebenfalls eine K-Basis von L. □

SATZ 24.3. *Sei*

$$\mathbb{R} \subseteq K$$

eine endliche Körpererweiterung der reellen Zahlen. Dann ist K isomorph zu $\mathbb{R}$ oder zu $\mathbb{C}$.

Beweis. Das reelle normierte Polynom $P \in \mathbb{R}[X]$ zerfällt über den komplexen Zahlen $\mathbb{C}$ nach dem Fundamentalsatz der Algebra in Linearfaktoren, d.h. es ist

$$P = \prod_j (X - \lambda_j)$$

mit $\lambda_j = a_j + b_j i \in \mathbb{C}$. Da P reelle Koeffizienten hat, stimmt es mit seinem komplex-konjugierten überein, d.h. es ist insgesamt

$$\prod_j (X - \lambda_j) \;=\; P \;=\; \overline{P} \;=\; \prod_j (X - \overline{\lambda_j}).$$

Wegen der Eindeutigkeit der Primfaktorzerlegung gibt es zu jedem j ein k mit $\overline{\lambda_j} = \lambda_k$. D.h. entweder, dass $\lambda_j \in \mathbb{R}$ ist, und dann liegt ein reeller Linearfaktor vor, oder aber $j \neq k$ und dann ist

$$(X - \lambda_j)(X - \overline{\lambda_j}) \;=\; (X - a_j - b_j i))(X - a_j + b_j i) \;=\; X^2 - 2a_j X + a_j^2 + b_j^2$$

ein reelles Polynom. In der reellen Primfaktorzerlegung von P kommen also nur lineare und quadratische Faktoren vor, und insbesondere haben im Reellen alle irreduziblen Polynome den Grad eins oder zwei.

Sei nun $\mathbb{R} \subseteq L$ eine endliche Körpererweiterung. Sei $\mathbb{R} \subset L$ und $x \in L$, $x \notin \mathbb{R}$. Dann ist x algebraisch über $\mathbb{R}$ und nach Satz 23.1 ist $\mathbb{R}[x] \cong \mathbb{R}[X]/(P)$ mit einem irreduziblen Polynom P (dem Minimalpolynom zu x). Das Polynom P besitzt in $\mathbb{C}$ Nullstellen, so dass es einen $\mathbb{R}$-Algebra-Homomorphismus $\mathbb{R}[X]/(P) \to \mathbb{C}$ gibt. Da beides reell-zweidimensionale Körper sind, muss eine Isomorphie vorliegen. Wir erhalten also eine endliche Körpererweiterung $\mathbb{C} \subseteq L$. Da $\mathbb{C}$ algebraisch abgeschlossen ist, muss nach Aufgabe 24.16 $\mathbb{C} = L$ sein. □

Die Gradformel

Satz 24.4. *Seien $K \subseteq L$ und $L \subseteq M$ endliche Körpererweiterungen. 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 erzeugen. Sei dazu $z \in M$. Wir schreiben

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

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

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

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

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

angenommen mit $c_{ij} \in K$. Wir schreiben dies als $0 = \sum_{j=1}^{m} () \, y_j$. 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 24.5. *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

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

eine Körpererweiterung von K nach Satz 15.1. 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 $\tilde{P}$ einen 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 24.6. 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. Ferner ist er eindeutig bestimmt, es gibt also bis auf Isomorphie nur einen Zerfällungskörper zu einem Polynom. Er wird mit $Z(F)$ bezeichnet. 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 24.7. *Es sei K ein Körper, $F \in K[X]$ ein Polynom und $L = Z(F)$ der Zerfällungskörper von F. Es sei $K \subseteq K' \subseteq L$ ein Zwischenkörper. Dann ist L auch ein Zerfällungskörper des Polynoms $F \in K'[X]$.*

Beweis. Das ist trivial. □

LEMMA 24.8. *Es sei K ein Körper, $F \in K[X]$ ein Polynom und $L = Z(F)$ der Zerfällungskörper von 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 23.4 endliche Körpererweiterungen und nach Satz 24.4 ist dann die Gesamtkörpererweiterung ebenfalls endlich. □

SATZ 24.9. *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*

$$\varphi\colon L_1 \longrightarrow L_2.$$

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 15.1 und nach Proposition 22.1 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 24.4 sind dann L_1 und L_2 Zerfällungskörper von $F \in K'[X]$. Nach Satz 24.4 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

$$\varphi\colon L_1 \longrightarrow L_2.$$

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