TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Mathematik Institut für Algebra, Professur für Algebra

ELEMENTE DER ALGEBRA UND ZAHLENTHEORIE

Prof. Dr. Arno Fehm

Sommersemester 2019

Autor : Eric Kunze
E-Mail : eric.kunze@mailbox.tu-dresden.de

Kapitel 1

KÖRPERERWEITERUNGEN

1 Körpererweiterungen

Definition 1.1

$L|K$ ist endlich erzeugt $\Leftrightarrow$ $a_1, \ldots, a_n \in L : L = K(a_1, \ldots, a_n)$ $L|K$ ist einfach $\Leftrightarrow$ ex. $a \in L : L = K(a)$

Bemerkung 1.2

(a) $L|K$ endlich $\Rightarrow$ $L|K$ endlich erzeugt.

(b) $K[a_1, \ldots, a_n]$ ist das Bild des Homomorphismus

$$\begin{cases} K[a_1, \ldots, a_n] & \to & L \\ f & \mapsto & f(a_1, \ldots, a_n) \end{cases}$$

und $K(a_1, \ldots, a_n) = \left\{ \frac{\alpha}{\beta} : \alpha, \beta \in K[a_1, \ldots, a_n], \beta \neq 0 \right\} \cong \operatorname{Quot}(K[a_1, \ldots, a_n])$

2 Algebraische Körpererweiterungen

Sei $L|K$ eine Körpererweiterung.

Definition 2.1 (!)

Sei $\alpha \in L$. Gibt es ein $0 \neq f \in K[X]$ mit $f(\alpha) = 0$, so heißt α **algebraisch** über K, andernfalls **transzendent** über K.

Beispiel 2.2

(a) $\alpha \in K$ $\Rightarrow$ α ist algebraisch über K (denn $f(\alpha) = 0$ für $f = X - \alpha \in K[X]$)

(b) $\sqrt{-1} \in \mathbb{Q}(\sqrt{-1})$ ist algebraisch über $\mathbb{Q}$ (denn $f(\sqrt{-1}) = 0$ für $f = X^2 + 1 \in \mathbb{Q}[X]$)
$\sqrt{-1} \in \mathbb{C}$ ist algebraisch über $\mathbb{R}$

Bemerkung 2.3

Sind $K \subseteq L \subseteq M$ Körper und $\alpha \in M$ algebraisch über K, so auch über L.

Lemma 2.4

Genau dann ist $\alpha \in L$ algebraisch über K, wenn $1, \alpha, \alpha^2, \ldots$ K-linear abhängig sind.

Beweis. Für $\lambda_0, \lambda_1, \dots \in K$, fast alle gleich Null, so ist

$$\sum_{i=0}^{\infty} \lambda_i \alpha^i \quad \Leftrightarrow \quad f(\alpha) = 0 \text{ für } f = \sum_{i=0}^{\infty} \lambda_i X^i \in K[X]$$

Lemma 2.5

Betrachte den Epimorphismus

$$\varphi_\alpha\colon \begin{cases} K[X] & \to & K[\alpha] \\ f & \mapsto & f(\alpha) \end{cases}$$

Genau dann ist α algebraisch über K, wenn $\operatorname{Ker}(\varphi_\alpha) \neq (0)$. In diesem Fall ist $\operatorname{Ker}(\varphi_\alpha) = (f_\alpha)$ mit einem eindeutig bestimmten irreduziblen, normierten $f_\alpha \in K[X]$.

Beweis. $K[X]$ Hauptidealring $\Rightarrow$ $\operatorname{Ker}(\varphi_\alpha) = (f_\alpha)$, $f_\alpha \in K[X]$, o.E. sei f_α normiert. Aus $K[\alpha] \subseteq L$ nullteilerfrei folgt, dass $\operatorname{Ker}(\varphi_\alpha)$ prim ist. Somit ist f_α prim und im Hauptidealring also auch irreduzibel. □

Definition 2.6

Sei $\alpha \in L$ algebraisch über K, $\operatorname{Ker}(\varphi_\alpha) = (f_\alpha)$ mit $f_\alpha \in K[X]$ normiert und irreduzibel.

(1) $\operatorname{MinPol}(\alpha \mid K) := f_\alpha$, das **Minimalpolynom** von α über K.

(2) $\deg(\alpha \mid K) := \deg(f_\alpha)$, der **Grad** von α über K.

Satz 2.7

Sei $\alpha \in L$.

(a) α transzendent über K

$\Rightarrow$ $K[\alpha] \cong K[X]$, $K(\alpha) \cong_K K(X)$, $[K(\alpha)\colon K] = \infty$.

(b) α algebraisch über K

$\Rightarrow$ $K[\alpha] = K(\alpha) \cong K[X]/\operatorname{MinPol}(\alpha|K)$, $[K(\alpha)\colon K)] = \deg(\alpha|K) < \infty$ und $1, \alpha, \ldots, \alpha^{\deg(\alpha|K)-1}$ ist K-Basis von $K(\alpha)$.

Beweis. (a) $\operatorname{Ker}(\varphi_\alpha) = (0)$ $\Rightarrow$ φ_α ist Isomorphismus (da zusätzlich injektiv)

$\Rightarrow$ $K(\alpha) \cong_K \operatorname{Quot}(K[\alpha]) \cong_K \operatorname{Quot}(K[X]) = K(X)$

$\Rightarrow$ $[K(\alpha)\colon K] = [K(X)\colon K] = \infty$

(b) Sei $f = f_\alpha = \operatorname{MinPol}(\alpha \mid K)$, $n = \deg(\alpha|K) = \deg(f)$.

- f irreduzibel $\Rightarrow$ $(f) \neq (0)$ prim $\overset{\text{GEO II.4.7}}{\Longrightarrow}$ (f) ist maximal
  $\Rightarrow$ $K[\alpha] \cong K[X]/(f)$ ist Körper $\Rightarrow$ $K[\alpha] = K(\alpha)$
- $1, \alpha, \ldots, \alpha^{n-1}$ sind K-linear unabhängig:

$$\sum_{i=0}^{n-1} \lambda_i \alpha^i = 0 \;\Rightarrow\; \sum_{i=0}^{n-1} \lambda_i X^i \in (f) \quad \overset{\deg f = n}{\Longrightarrow} \quad \lambda_i = 0 \;\; \forall i$$

$1, \alpha, \ldots, \alpha^{n-1}$ ist Erzeugendensystem: Für $g \in K[X]$ ist

$$g = q \cdot f + r \text{ mit } q, r \in K[X] \text{ und } \deg(r) < \deg(f) = n$$

und

$$g(\alpha) = q(\alpha) \underbrace{f(\alpha)}_{=0} + r(\alpha) = r(\alpha)$$

somit $K[X] = \operatorname{Im}(\varphi_\alpha) = \{g(\alpha)\colon g \in K[X]\} = \{r(\alpha)\colon r \in K[X], \deg(r) < n\} = \sum_{i=0}^{n-1} K \cdot \alpha^i$ □

Beispiel 2.8

(a) $p \in \mathbb{Z}$ prim $\Rightarrow$ $\sqrt{p} \in \mathbb{C}$ ist algebraisch über $\mathbb{Q}$.
Da $f(X) = X^2 - p$ irreduzibel in $\mathbb{Q}[X]$ ist (GEO II.7.3), ist $\operatorname{MinPol}\left(\sqrt{p} \mid \mathbb{Q}\right) = X^2 - p$, $[\mathbb{Q}(\sqrt{p})\colon \mathbb{Q}] = 2$.

(b) Sei $\zeta_p = e^{2\pi i/p} \in \mathbb{C}$ ($p \in \mathbb{N}$ prim). Da $\Phi_p = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1 \in \mathbb{Q}[X]$ irreduzibel in $\mathbb{Q}[X]$ ist (GEO II.7.9), ist $\operatorname{MinPol}(\zeta_p \mid \mathbb{Q}) = \Phi_p$, $[\mathbb{Q}(\zeta_p)\colon \mathbb{Q}] = p - 1$. Daraus folgt schließlich

$$[\mathbb{C}\colon \mathbb{Q}] \geq [\mathbb{Q}(\zeta_p)\colon \mathbb{Q}] = p-1 \ \forall p \ \Rightarrow \ [\mathbb{C}\colon \mathbb{Q}] = \infty \ \Rightarrow \ [\mathbb{R}\colon \mathbb{Q}] = \infty.$$

(c) $e \in \mathbb{R}$ ist transzendent über $\mathbb{Q}$ (Hermite 1873), $\pi \in \mathbb{R}$ ist transendent über $\mathbb{Q}$ (Lindemann 1882). Daraus folgt: $[\mathbb{R}\colon \mathbb{Q}] \geq [\mathbb{Q}(\pi)\colon \mathbb{Q}] = \infty$. Jedoch ist unbekannt, ob z.B. $\pi + e$ transzendent ist.

Definition 2.9

$L|K$ ist **algebraisch** $:\Leftrightarrow$ jedes $\alpha \in L$ ist algebraisch über K.

Satz 2.10

$L|K$ endlich $\Rightarrow$ $L|K$ algebraisch.

Beweis. $\alpha \in L$, $[L\colon K] = n \Rightarrow 1, \alpha, \ldots, \alpha^n$ K-linear abhängig $\overset{2.4}{\Rightarrow}$ α algebraisch über K. □

Korollar 2.11

Ist $L = K(\alpha_1, \ldots, \alpha_n)$ mit $\alpha_1, \ldots, \alpha_n$ algebraisch über K, so ist $L|K$ endlich, insbesondere algebraisch.

Beweis. Vollständige Induktion nach n:

(IA) $n = 0:$ ✓

(IS) $n > 0: \ K_1 := K(\alpha_1, \ldots, \alpha_{n-1})$

$\Rightarrow \ L = K_1(\alpha_n)$, α_n algebraisch über K_1 (2.3)

$\Rightarrow \ [L\colon K] = \underbrace{[K_1(\alpha_n)\colon K_1]}_{<\infty \text{ nach } 2.7} \cdot \underbrace{[K_1 : K]}_{<\infty \text{ nach IH}}$ □

Korollar 2.12

Es sind äquivalent:

(1) $L|K$ ist endlich.

(2) $L|K$ ist endlich erzeugt und algebraisch.

(3) $L = K(\alpha_1, \ldots, \alpha_n)$ mit $\alpha_1, \ldots, \alpha_n$ algebraisch über K.

Beweis. (1) $\Rightarrow$ (2): 1.15 und 2.10

(2) $\Rightarrow$ (3): trivial

(3) $\Rightarrow$ (1): 2.11 □

Bemerkung 2.13

Nach 2.7 ist

$$\alpha \text{ algebraisch über } K \ \Leftrightarrow \ K[\alpha] = K(\alpha)$$

Direkter Beweis für ($\Rightarrow$):

Sei $0 \neq \beta \in K[\alpha]$. Daraus folgt, dass $f(\beta) = 0$ für ein irreduzibles $0 \neq f = \sum_{i=0}^n a_i X^i \in K[X]$. Durch Einsetzen von β und Division durch β erhält man (auch wegen der aus der Irreduzibilität folgenden Bedingung $a_0 \neq 0$)

$$\beta^{-1} = -a_0^{-1}(a_1 + a_2\beta + \cdots + a_n\beta^{n-1}) \in K[\beta] \subseteq K[\alpha]$$