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

Inhaltsverzeichnis

Kapitel I
KÖRPERERWEITERUNGEN

1 Körpererweiterungen

Seien K, L, M Körper.

Bemerkung 1.1

In diesem Kapitel bedeutet "Ring" *immer* kommutativer Ring mit Einselement, und ein Ringhomomorphismus bildet stets das Einselement auf das Einselement ab. Insbesondere gibt es für jeden Ring einen eindeutig bestimmten Ringhomomorphismus $\mathbb{Z} \to R$.

Bemerkung 1.2

(a) Ein **Körper** ist ein Ring R, in dem eine der folgenden äquivalenten Bedingungen gilt:
   (1) $0 \neq 1$ und jedes $0 \neq x \in R$ ist invertierbar
   (2) $R^\times = R \setminus \{0\}$
   (3) R hat genau zwei Hauptideale (nämlich (0) und (1))
   (4) (0) ist ein maximales Ideal von R
   (5) (0) ist das einzige echte Ideal von R
   (6) (0) ist das einzigste Primideal von R

(b) Insbesondere sind Körper **nullteilerfrei**, weshalb $\mathrm{Ker}(\mathbb{Z} \to K)$ prim ist.

(c) Aus (5) folgt: Jeder Ringhomomorphismus $K \to L$ ist injektiv (Beweisidee: Ker ist ein Ideal, muss das Nullideal sein und somit auch schon trivial)

(d) Der Durchschnitt einer Familie von Teilkörpern von K ist wieder ein Teilkörper von K.

Definition 1.3 (Charakteristik)

Die **Charakteristik** von K, $\mathrm{char}(K)$, ist das $p \in \{0, 2, 3, 5, 7, \ldots\}$ mit $\mathrm{Ker}(\mathbb{Z} \to K) = (p)$.

Beispiel 1.4

(a) $\mathrm{char}(\mathbb{Q}) = 0$ und $\mathrm{char}(\mathbb{F}_p) = (p)$ (p Primzahl), wobei $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

(b) Ist $K_0 \subseteq K$ Teilkörper, so ist $\mathrm{char}(K_0) = \mathrm{char}(K)$.

Definition 1.5 (Primkörper)

Der **Primkörper** von K ist der kleinste Teilkörper von K (existiert nach Bemerkung 1.2(d)).

Satz 1.6

Sei $\mathbb{F}$ der Primkörper von K.

(a) $\mathrm{char}(K) = 0 \;\Leftrightarrow\; \mathbb{F} \cong \mathbb{Q}$

(b) $\mathrm{char}(K) = p > 0 \;\Leftrightarrow\; \mathbb{F} \cong \mathbb{F}_p$

Beweis. **($\Leftarrow$)** Beispiel 1.4

($\Rightarrow$) $\mathrm{Im}(\mathbb{Z} \to K) \subseteq \mathbb{F}$ und $\mathrm{Im}(\mathbb{Z} \to K) \cong \mathbb{Z}/_{\mathrm{Ker}(\mathbb{Z}\to K)}$

   (a) $\mathrm{Im}(\mathbb{Z} \to K) \cong \mathbb{Z}/_{(0)} \cong \mathbb{Z} \;\Rightarrow\; \mathbb{F} = \mathrm{Quot}(\mathrm{Im}(\mathbb{Z} \to K)) \cong \mathrm{Quot}(\mathbb{Z}) \cong \mathbb{Q}$

   (b) $\mathrm{Im}(\mathbb{Z} \to K) \cong \mathbb{Z}/_{(p)} \cong \mathbb{F}_p$ ist Teilkörper von K $\Rightarrow \mathbb{F} = \mathrm{Im}(\mathbb{Z} \to K) \cong \mathbb{F}_p$ $\square$

Definition 1.7 (Körpererweiterung)

Ist K ein Teilkörper von L, so nennt man L eine **Körpererweiterung** von K, auch geschrieben $L \mid K$.

Definition 1.8 (K-Homomorphismus)

Seien $L_1 \mid K$ und $L_2 \mid K$ Körpererweiterungen.

(1) Ein Ringhomomorphismus $\varphi\colon L_1 \to L_2$ ist ein K-Homomorphismus, wenn $\varphi|_K = \mathrm{id}_K$ (i.Z. $\varphi\colon L_1 \to_K L_2$)

(2) $\mathrm{Hom}_K(L_1, L_2) = \{\varphi \mid \varphi\colon L_1 \to L_2 \text{ ist } K\text{-Homomorphismus}\}$

(3) L_1 und L_2 sind K-isomorph (i.Z. $L_1 \cong_K L_2$), wenn es einen Isomorphismus $\varphi \in \mathrm{Hom}_K(L_1, L_2)$ gibt.

Bemerkung 1.9

Ist $L|K$ eine Körpererweiterung, so wird L durch Einschränkung der Multiplikation zu einem K-Vektorraum.

Definition 1.10 (Körpergrad)

$[L : K] := \dim_K(L) \in \mathbb{N} \cup \{\infty\}$, der **Körpergrad** der Körpererweiterungen $L|K$.

Beispiel 1.11

(a) $[K : K] = 1$

(b) $[\mathbb{C} : \mathbb{R}] = 2$ (Basis $(1, i)$, aber Index $(\mathbb{C} : \mathbb{R}) = \infty$)

(c) $[\mathbb{R} : \mathbb{Q}] = \infty$ (mit Abzählbarkeitsargument oder siehe §2)

(d) $[K(x) : K] = \infty$ $(K(X) = \mathrm{Quot}(K[X]))$ (vgl. GEO II.8)

Satz 1.12

Für $K \subseteq L \subseteq M$ Körper ist

$$[M : K] = [M : L] \cdot [L : K]$$

("Körpergrad ist multiplikativ")

Beweis. *Behauptung:* Sei $x_1, \dots, x_n \in L$ K-linear unabhängig und $y_1, \dots, y_m \in M$ L-linear unabhängig. Dann ist auch $\{x_i y_i : i = 1, \dots, n; j = 1, \dots, m\}$ K-linear unabhängig.

Beweis: $\sum_{i,j} \lambda_{ij} x_i y_j = 0$ mit $\lambda_{ij} \in K$

$$\Longrightarrow \sum_j \underbrace{\left(\sum_i \lambda_{ij} x_i\right)}_{\in L} y_j = 0 \quad \overset{y_j\, L\text{-lin. unabh.}}{\Longrightarrow} \quad \sum_i \lambda_{ij} x_i = 0 \quad \forall j \quad \overset{y_j\, K\text{-lin. unabh.}}{\Longrightarrow} \quad \lambda_{ij} = 0 \quad \forall i \ \forall j$$

- $[L : K] = \infty$ oder $[M : L] = \infty \quad \Rightarrow \quad [M : K] = \infty \checkmark$
- $[L : K] = n, [M : L] = m$ mit $n, m < \infty$
  $(x_1, \dots, x_n)$ sei Basis des K-Vektorraum L und $(y_1, \dots, y_m)$ Basis des L-Vektorraums M
  $\Rightarrow \quad \{x_i y_j : i = 1, \dots, n; j = 1, \dots, m\}$ K-linear unabhängig und

$$\sum_{i,j} K x_i y_j = \sum_j \underbrace{\left(\sum_i K x_i\right)}_{=L} y_j = M$$

  also ist $\{x_i y_j : i = 1, \dots, n; j = 1, \dots, m\}$ Basis von M □

Definition 1.13

$L|K$ endlich $\quad :\Leftrightarrow \quad [L : K] < \infty$.

Definition 1.14 (Unterring, Teilkörper)

Sei $L|K$ eine Körpererweiterung $a_1, a_2, \ldots, a_n \in L$.

(1) $K[a_1, \ldots, a_n]$ ist der kleinste **kleinste Unterring** von L, der $K \cup \{a_1, \ldots, a_n\}$ enthält ("von $a_1, \ldots, a_n$ über K erzeugt")

(2) $K(a_1, \ldots, a_n)$ ist **kleinster Teilkörper** von L, der $K \cup \{a_1, \ldots, a_n\}$ enthält ("von $a_1, \ldots, a_n$ über K erzeugt", "$a_1, \ldots, a_n$" zu K adjungieren")

(3) $L|K$ ist **endlich erzeugt** $:\Leftrightarrow$ $a_1, \ldots, a_n \in L$ mit $L = K(a_1, \ldots, a_n)$

(4) $L|K$ ist **einfach** $:\Leftrightarrow$ ex. $a \in L$ mit $L = K(a)$

Bemerkung 1.15

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

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, ist $\sum_{i=0}^{\infty} \lambda_i \alpha^i$ $\Leftrightarrow$ $f(\alpha) = 0$ 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 $\mathrm{Ker}(\varphi_\alpha) \neq (0)$. In diesem Fall ist $\mathrm{Ker}(\varphi_\alpha) = (f_\alpha)$ mit einem eindeutig bestimmten irreduziblen, normierten $f_\alpha \in K[X]$.

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

Definition 2.6

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

(1) $\mathrm{MinPol}(\alpha \mid K) := f_\alpha$, 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

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

(b) α algebraisch über K

$\Rightarrow\ K[\alpha] = K(\alpha) \cong K[X]/\mathrm{MinPol}(\alpha|K) \quad , \quad [K(\alpha)\colon K)] = \deg(\alpha|K) < \infty \quad$ und

$1, \alpha, \dots, \alpha^{\deg(\alpha|K)-1}$ ist K-Basis von $K(\alpha)$.

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

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

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

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

- 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 $\ \Rightarrow\ K[\alpha] = K(\alpha)$
- $1, \alpha, \dots, \alpha^{n-1}$ sind K-linear unabhängig:

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

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

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 $\mathrm{MinPol}\left(\sqrt{p} \mid \mathbb{Q}\right) = X^2 - p$, $[\mathbb{Q}(\sqrt{p})\colon \mathbb{Q}] = 2$.

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

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

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 $a_0 \neq 0$)

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