Algebra und Zahlentheorie SS 2019

Dozent: Prof. Dr. Arno Fehm

17. April 2019

Inhaltsverzeichnis

Vorwort

Motivation und Einführung

Kapitel I

Körper

1. Körpererweiterungen

Sei 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

(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**

1. $\mathrm{char}(\mathbb{Q}) = 0$ und $\mathrm{char}(\mathbb{F}_p) = (p)$ ($p =$ Primzahl), wobei $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$
2. 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) $\operatorname{char}(K) = 0 \Leftrightarrow \mathbb{F} \cong \mathbb{Q}$

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

Beweis. "$\Leftarrow$": Beispiel 1.4
"$\Rightarrow$": $\operatorname{Im}(\mathbb{Z} \to K) \subseteq \mathbb{F}$ und $\operatorname{Im}(\mathbb{Z} \to K) \cong \mathbb{Z}/\operatorname{Ker}(\mathbb{Z} \to K)$

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

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

Definition 1.7 (Körpererweiterung)
Ist K ein Teilkörper von L, so nennt man L eine Köpererweiterung 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. $\varphi : L_1 \to L_2$)
2. $\operatorname{Hom}_K(L_1, L_2) = \{\varphi \mid \varphi : L_1 \to L_2 \text{ ist } K\text{-Homomorphismus}\}$
3. L_1 und L_2 sind K-isomorph (i.Z. $L_1 \cong L_2$), wenn es einen Isomorphismus: $\varphi \in \operatorname{Hom}_K(L_1, L_2)$ gibt.

▶ **Bemerkung 1.9**
$L \mid K$ 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 $L \mid K$.

■ **Beispiel 1.11**

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

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

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

(d) $[K(x) : K] = \infty$ ($K(x) = \operatorname{Quot}(K[x])$ (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
$\Rightarrow x_i y_j, i \in \{1, \dots, n\}, j \in \{1, \dots, m\}$ K-linear unabhängig.
Beweis: $\sum_{i,j} \lambda_{ij} x_i y_j = 0$ mit $\lambda_{ij} \in K$

$$\Rightarrow \sum_j \underbrace{\left(\sum_i \lambda_{ij} x_i\right)}_{\in L} y_j = 0 \xRightarrow{y_j\, L\text{-l.u.}} \sum_i \lambda_{ij} x_i = 0 \quad \forall j \xRightarrow{y_j\, K\text{-l.u.}} \lambda_{ij} = 0 \quad \forall i, \forall j$$

- $[L : K] = \infty$ oder $[M : L] = \infty \Rightarrow [M : K] = \infty$
- $[L : K] = n, [M : L] = m < \infty$
  $(x_1, \ldots, x_n)$ Basis des K-Vektorraum L und $(y_1, \ldots, y_m)$ Basis des L-Vektorraums M
  $\Rightarrow \{x_i y_j : i = 1, \ldots, n; j = 1, \ldots, m\}$ K-linear unabhängig und
  $\sum_{i,j} K x_i y_j = \sum_j \left(\sum_i \lambda_{ij} x_i\right) y_j = M$, also ist
  $\{x_i y_j : i = 1, \ldots, n; j = 1, \ldots, m\}$ Basis von M □

Definition 1.13 (Körpergrad endlich)
$L \mid K$ endlich $:\Leftrightarrow [L : K] < \infty$.

Definition 1.14 (Unterring, Teilkörper)
Sei $L \mid K$ eine Körpererweiterung $a_1, a_2, \ldots, a_n \in L$.

1. $K[a_1, \ldots, a_n]$ ist kleinster Unterring von L, der $K \cup \{a_1, \ldots, a_n\}$ enthält ("$a_1, \ldots, a_n$ 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 erzeugte", "$a_1, \ldots, a_n$" zu K adjungieren)
3. $L|K$ ist endlich erzeugt $:\Leftrightarrow a_1, \ldots, a_n \in L : L = K(a_1, \ldots, a_n)$
4. $L|K$ ist einfach $:\Leftrightarrow$ existiert $a \in L : L = K(a)$

▶ **Bemerkung 1.15**

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

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

$$\begin{cases} K[x_1, \ldots, x_n] & \to L \\ f & \mapsto f(a_1, \ldots, a_n) \end{cases}$$

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

2. Algebraische Körpererweiterungen

Sei $L \mid K$ eine Körpererweiterung.

Definition 2.1 (algebraisch, transzendent)
Sei $\alpha \in L$. Gibt es ein $0 \neq f \in K$ mit $f(\alpha) = 0$, so heißt α algebraisch über K, andernfalls transzendent über K.

■ **Beispiel 2.2**

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

(b) $\sqrt{-1} \in \mathbb{Q}(\sqrt{-1})$ ist algebraisch über $\mathbb{Q}$ (denn $f(\sqrt{-1}) = 0$ für $f = X^2 + 1 \in \mathbb{Q}$)
$\sqrt{-1} \in \mathbb{C}$ 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 $1, \alpha, \alpha^2, \dots$ K-linear abhängig sind.

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

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

□

Lemma 2.5
Betrachte den Epimorphismus

$$\varphi_\alpha : \begin{cases} K[x] & \to K[\alpha] \\ f & \mapsto f(\alpha). \end{cases}$$

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 $f_\alpha \in K$.

Beweis. K Hauptidealring $\Rightarrow \operatorname{Ker}(\varphi_\alpha) = (f_\alpha)$, $f_\alpha \in K$, 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 (Monimalpolynom, Grad)
Sei $\alpha \in L$ algebraisch über K, $\operatorname{Ker}(\varphi_\alpha) = (f_\alpha)$ mit $f_\alpha \in K$ normiert und irreduzibel.

1. $\operatorname{MinPol}(\alpha \mid K) := f_\alpha$, das Minimalpolynom von α über K.
2. $\deg(\alpha \mid K) :\Leftrightarrow \deg(f_\alpha)$, der Grad von α über K.

Satz 2.7
Sei $\alpha \in L$.

1. α transzendent über K
   $\Rightarrow K[\alpha] \cong K$, $K(\alpha) \cong_K K(X)$, $[K(\alpha) : K] = \infty$.

2. α algebraisch über K
   $\Rightarrow K[\alpha] = K(\alpha) \cong K/\operatorname{MinPol}(\alpha \mid K)$, $[K(\alpha)\colon K)] = \deg(\alpha \mid K) < \infty$ und
   $1, \alpha, \dots, \alpha^{\deg(\alpha|K)-1}$ ist K-Basis von $K(\alpha)$.

Beweis. (a) $\operatorname{Ker}(\varphi_\alpha) = (0) \Rightarrow \varphi_\alpha$ ist Isomorphismus (da zusätzlich injektiv)
$\Rightarrow K(\alpha) \cong_K \operatorname{Quot}(K[\alpha]) \cong_K \operatorname{Quot}(K) = K(X)$
$\Rightarrow [K(\alpha)\colon K] = [K(x)\colon K] = \infty$

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

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

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

$1, \alpha, \dots, \alpha^{n-1}$ ist Erzeugendensystem: Für $g \in K$ ist

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

und

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

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

■ **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 $\mathbb{Q}$ ist (GEO II.7.3), ist $\operatorname{MinPol}(\sqrt{p} : \mathbb{Q}) = X^2 - p$, $[\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = 2$.

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

(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: $[R : \mathbb{Q}] \geq [\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$. Jedoch ist unbekannt, ob z.B. $\pi + e$ transzendent ist.

Definition 2.9
$L \mid K$ ist algebraisch :⇔ jedes $\alpha \in L$ ist algebraisch über K.

Satz 2.10
$L \mid K$ endlich $\Rightarrow L \mid K$ algebraisch.

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

Folgerung 2.11
Ist $L = K(\alpha_1, \dots, \alpha_n)$ mit $\alpha_1, \dots, \alpha_n$ algebraisch über K, so ist $L \mid K$ endlich, insbesondere algebraisch.

Beweis. Induktion nach n:

- $n = 0$: ✓
- $n > 0$: $K_1 := K(\alpha_1, \dots, \alpha_{n-1})$
  $\Rightarrow L = K_1(\alpha_n)$, α_n algebraisch über K_1 (Bemerkung 2.3)
  $\Rightarrow [L : K] = \underbrace{[K_1(\alpha_n) : K_1]}_{<\infty \text{ nach Satz } 2.7} \cdot \underbrace{[K_1 : K]}_{<\infty \text{ nach IH}}$ □

Folgerung 2.12
Es sind äquivalent:

1. $L \mid K$ ist endlich.
2. $L \mid K$ ist endlich erzeugt und algebraisch.
3. $L = K(\alpha_1, \dots, \alpha_n)$ mit $\alpha_1, \dots, \alpha_n$ algebraisch über K.

Beweis.
- (1) $\Rightarrow$ (2): Bemerkung 1.15 und Satz 2.10
- (2) $\Rightarrow$ (3): trivial
- (3) $\Rightarrow$ (1): Folgerung 2.11 □

▶ **Bemerkung 2.13**
Nach Satz 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 $0 \neq f = \sum_{i=0}^{n} a_i X^i \in K$. Durch Einsetzen von β und Division durch β erhält man (auch wegen der aus der Irreduzibilität

$$\overset{a_0 \neq 0}{\Longrightarrow} \beta^{-1} = -a_0^{-1}(a_1 + a_2\beta + \dots + a_n\beta^{n-1}) \in K[\beta] \subseteq K[\alpha]$$

Satz 2.14
Seien $K \subseteq L \subseteq M$ Körper. Dann gilt:

$$M \mid K \text{ algebraisch } \Leftrightarrow M \mid L \text{ algebraisch und } L \mid K \text{ algebraisch}$$

Beweis. ($\Rightarrow$) klar, siehe Bemerkung 2.3.
($\Leftarrow$) Sei $\alpha \in M$. Schreibe $f = \mathrm{MinPol}(\alpha \mid L) = \sum_{i=0}^{n} a_i x^i$, $\quad L_0 := K(a_0, \dots, a_n)$
$\Rightarrow f \in L_0[x]$

$\Rightarrow [L_0(\alpha) : L_0] \leq \deg(f) \leq \infty$

$\Rightarrow [K(\alpha : K)] \leq [K(a_0, \dots, a_n, \alpha) : K] = \underbrace{[L_0(\alpha) : L_0]}_{<\infty} \underbrace{[L_0 : K]}_{< \text{ nach } 2.7}$

$\Rightarrow \alpha$ abgebraisch über K

$\overset{\alpha \text{ bel.}}{\Rightarrow} M \mid K$ algebraisch. □

Folgerung 2.15
$\tilde{K} = \{\alpha \in L\colon \alpha$ algebraisch über $K\}$ ist ein Körper, und ist $\alpha \in L$ algebraisch über $\tilde{K}$, so ist schon $\alpha \in \tilde{K}$.

Beweis.
- $\alpha, \beta \in \tilde{K}$:
  $\Rightarrow K(\alpha, \beta) \mid K$ endlich, insbesondere algebraisch
  $\Rightarrow \alpha + \beta, \alpha - \beta, \alpha \cdot \beta, \alpha^{-1} \in K(\alpha, \beta)$ alle algebraisch über K, also $K(\alpha, \beta) \subseteq \tilde{K}$.
- $\alpha \in L$ algebraisch über $\tilde{K}$:
  $\Rightarrow \tilde{K}(\alpha) \mid \tilde{K}$ algebraisch
  $\Rightarrow \tilde{K} \mid K$ algebraisch $\overset{2.14}{\Rightarrow} \tilde{K}(\alpha \mid K)$ algebraisch, insbesondere $\alpha \in \tilde{K}$. □

Definition 2.16 (relative algebraische Abschluss)
$\tilde{K} = \{\alpha \in L\colon \alpha$ algebraisch über $K\}$ heißt der relative algebraische Abschluss von K in L.

■ **Beispiel 2.17**
$\tilde{\mathbb{Q}} = \{\alpha \in \mathbb{C}\colon \alpha$ algebraisch über $K\}$ ist ein Körper, der Körper der algebraischen Zahlen. Es ist $[\tilde{\mathbb{Q}}, \mathbb{Q}] = \infty$, z.B. da $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$ für jedes p prim. (algebraische Erweiterung die nicht endlich ist.)

Anhang

Index