III Körpererweiterungen

14. Grundbegriffe

Def. (a) Ist $K \subseteq L$ ein Unterkörper eines Körpers L, so heisst L eine Körpererweiterung von K und wir schreiben $L:K$.

(b) Sind $M:L$ und $L:K$ Körpererweiterungen, so heisst L ein Zwischenkörper der Körpererweiterung $M:K$.

(c) Ist $L:K$ eine Körpererweiterung und $A \subseteq L$ eine Teilmenge von L, so ist:

- $K[A]$ der Durchschnitt aller Unterringe von L welche K und A enthalten (kl. Ring mit $A \& K$).
- $K(A)$ der Durchschnitt aller Unterkörper von L welche K und A enthalten (kl. Körper mit $A \& K$).

Ist $A = \{a_0, \dots, a_n\}$ endlich, so sei $K[a_0, \dots, a_n] := K[A]$ und $K(a_0, \dots, a_n) := K(A)$.

(d) Eine Körpererweiterung $L:K$ heisst einfach, wenn ein $a \in L$ existiert mit $L = K(a)$; a heisst primitives Element der Körpererweiterung.

(e) Ist $L:K$ eine Körpererweiterung, so ist L ein Vektorraum über K (d.h. L sind die Vektoren und K ist der Körper). Der Grad der Körpererweiterung $L:K$ ist die Dimension von L als K-Vektorraum und wird mit $[L:K]$ bezeichnet, d.h. $[L:K] = \dim_K L$. Ist $[L:K]$ endlich, so heisst $L:K$ eine endliche Körpererweiterung.

Bsp.
- $[\mathbb{R} : \mathbb{Q}]$ ist unendlich (siehe Aufgabe 86.(b)).
- $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$; es gilt $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$.

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$$

$$\frac{1}{\underbrace{a+b\sqrt{2}}_{\neq 0}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \underbrace{\frac{a}{a^2-2b^2}}_{\in \mathbb{Q}} + \underbrace{\frac{-b}{a^2-2b^2}}_{\in \mathbb{Q}} \cdot \sqrt{2}$$

Gradsatz für Körpererweiterungen 14.1 Sind $M:L$ und $L:K$ Körpererweiterungen, so ist $[M:K] = [M:L] \cdot [L:K]$.

Beweis: Ist $[M:L] = \infty$ oder $[L:K] = \infty$, so ist $[M:K] = \infty$.

Sei nun $[M:L] = n$ und $[L:K] = m$ mit $n, m \in \mathbb{N} \setminus \{0\}$.

Sei $x_1, \ldots, x_m \in L$ eine Basis des VR L über K und sei $y_1, \ldots, y_n \in M$ ——— " ——— M über L.

- Für jedes $\ell \in L$ gilt $\ell = \sum_{i=1}^{m} k_i x_i$ mit $k_i \in K$; analog: für jedes $v \in M$ gilt $v = \sum_{j=1}^{n} \ell_j y_j$ mit $\ell_j \in L$.
- Somit ist $v = \sum_{j=1}^{n} \big(\underbrace{\sum_{i=1}^{m} k_{i,j} x_i}_{= \ell_j}\big) \cdot y_j = \sum_{j=1}^{n} \sum_{i=1}^{m} \underbrace{k_{i,j}}_{\in K} \underbrace{(x_i \cdot y_j)}_{\in M}$,

also $[M:K] \leq n \cdot m$.

- Andererseits folgt aus $\sum_i x_i \cdot \sum_j k_{i,j} \cdot y_j = 0$, weil die x_i's lin. unabh. sind, $\sum_j k_{i,j} \cdot y_j = 0$ (für alle i), und weil die y_j's lin. unabh. sind ist für alle i,j: $k_{i,j} = 0$.
- Somit ist $\sum_{i,j} k_{i,j}(x_i \cdot y_j) = 0 \iff k_{i,j} = 0$, also sind die $x_i \cdot y_j$ lin. unabh. und $[M:K] \geq n \cdot m$.

⊣

Erinnerung:

- **Kor. 12.4:** Sei S ein komm. Ring, $R \subseteq S$ ein Unterring, und $s_0 \in S$. Dann ex. ein Ideal $\mathfrak{a}_{s_0} \subseteq R[X]$ mit $\mathfrak{a}_{s_0} \cap R = \{0\}$ und $R[X]/\mathfrak{a}_{s_0} \cong R[s_0]$.

- Def. Ist $\mathfrak{a}_{s_0}$ wie im Beweis von Kor. 12.4 und $\mathfrak{a}_{s_0} \neq (0)$, so heisst s_0 algebraisch über R, sonst heisst s_0 transzendent über R.
- Thm. 12.8 Ist K ein Körper, so ist $K[X]$ ein Hauptidealring.

Als Folgerung erhalten wir:

Für $L:K$ eine Körpererweiterung ($K \subseteq L$ Unterring) und $s_0 \in L$ ist $\mathfrak{a}_{s_0} = (f)$ (Hauptideal) und $K[X]/(f) \cong K[s_0]$.

Def. Sei $L:K$ eine Körpererweiterung. Dann heisst $L:K$ algebraisch, falls jedes Element $a \in L$ algebraisch über K ist; andernfalls heisst $L:K$ transzendent.

Bsp. $\mathbb{C}:\mathbb{R}$ ist alg. ; $\mathbb{Q}(e):\mathbb{Q}$ ist transzendent ; endl. Erw. sind alg. (später)

Satz 14.2 Sei $L:K$ eine Körpererweiterung und $a \in L$ sei transzendent über K. Dann existiert ein Isomorphismus

$$\varphi : K(a) \longrightarrow K(X) := \mathrm{Quot}(K[X])$$

Beweis: Sei $a \in L$ transzendent über K. Mit Kor. 12.4 ex. Isomorphismus

$$\varphi_a : K[X] \longrightarrow K[a] \subseteq L$$
$$p \longmapsto p(a)$$

D.h. $K(X) = \mathrm{Quot}(K[X]) \cong \mathrm{Quot}(K[a])$

Weiter gilt: $K[a] \subseteq \underbrace{\mathrm{Quot}(K[a])}_{\text{kl. Körper der } K \text{ und } a \text{ enthält}} \subseteq L$

Also $\mathrm{Quot}(K[a]) = K(a)$ und somit $K(a) \cong K(X)$.

$\dashv$

Satz 14.3 Sei $L:K$ eine Körpererweiterung und $a \in L$ algebraisch über K. Dann gilt:

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

(b) $K(a) \cong K[X]/(f)$ mit einem eindeutig bestimmten irred. normierten ($a_n = 1$) Polynom $f \in K[X]$.

(c) $[K(a):K] = \text{grad}(f) =: n$

(d) $1, a^1, \dots, a^{n-1}$ ist Basis von $K(a)$ als K-Vektorraum.

Def. Ist $L:K$ eine Körpererweiterung und $a \in L$ alg. über K, so heisst das Polynom f aus (b) das Minimalpolynom von a über K.

Bem. Minimalpolynome sind also normiert und irreduzibel.

Beweis von Satz 14.3:

zu (a) und (b): Mit Kor. 12.4 & Thm. 12.8 ist $K[X]/(f) \cong K[a]$ für ein Polynom $f \in K[X]$, $f \neq 0$, f normiert.

- Da $K[a] \subseteq L$, ist $K[a]$ ein Integritätsring und somit ist auch $K[X]/(f)$ ein Integritätsring (weil $K[a] \cong K[X]/(f)$).
- Nach Definition ist somit (f) ein Primideal in $K[X]$.
- Weil $K[X]$ Integritätsring ist (K ist ein Körper) und (f) ein Primideal ist, ist mit Lem. 13.1.(b), (f) ein Primelement und mit Lem. 13.1.(a) ist f irreduzibel.
- Da K ein Körper ist, ist mit Thm. 12.8 $K[X]$ ein Hauptidealring und aus Lem. 13.4 folgt, dass (f) ein maximales Ideal ist (beachte: f ist irreduzibel).
- Weil (f) ein max. Ideal ist folgt mit Prp. 11.2, dass $K[X]/(f)$ ein Körper ist.
- Somit haben wir $K[X]/(f) \cong K[a]$ ist ein Körper, d.h. $K[a] = K(a)$.