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 (Übung).

• $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$; 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 $x_1,\dots,x_m\in L$ eine Basis des VR L über K und sei $y_1,\dots,y_n\in M$ ——— " ——— M über L.

• Für jedes $l\in L$ gilt $l=\sum_{i=1}^{m}k_i x_i$ mit $k_i\in K$; analog: für jedes $v\in M$ gilt $v=\sum_{j=1}^{n}l_j y_j$ mit $l_j\in L$.

• Somit ist $v=\sum_{j=1}^{n}\underbrace{\left(\sum_{i=1}^{m}k_{i,j}x_i\right)}_{=l_j}\cdot y_j=\sum_{j=1}^{n}\sum_{i=1}^{m}\underbrace{k_{i,j}}_{\in K}\underbrace{(x_i\cdot y_j)}_{\in M}$,

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

• Andererseits folgt aus $\sum_j y_j\cdot\sum_i k_{i,j}x_i=0$, weil die y_j's lin. unabh. sind, $\sum_i k_{i,j}x_i=0$ (für alle i), und weil die x_i's lin. unabh. sind ist für alle i,j: $k_{i,j}=0$.

• Somit ist $\sum_{i,j}k_{i,j}(x_i\cdot y_j)=0 \Leftrightarrow k_{i,j}=0$, 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 $R[X]/\mathfrak{a}_{s_0}\cong R[s_0]$.

- <u>Def.</u> 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.
- <u>Thm. 12.8</u> 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 $K[X]/(f) \cong K[s_0]$.

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

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

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

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

<u>Beweis:</u> 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. $K(X) = \operatorname{Quot}(K[X]) \cong \operatorname{Quot}(K[a])$

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

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

$\dashv$

<u>Satz 14.3</u> 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.

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

<u>Bem.</u> Minimalpolynome sind also normiert und irreduzibel.

<u>Beweis von Satz 14.3:</u>

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
  $d = \text{ggT}(a,b);\ (d) = (a,b)$
  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. $K[a] = K(a)$.

zu (c) und (d): zu zeigen ist nur (d), (c) folgt aus $n = \mathrm{grad}(f)$.

(i) $1, a^1, \ldots, a^{n-1}$ erzeugen $K(a) = K[a]$:

- Sei $r \in K(a) = K[a]$. Dann ex. $p \in K[X]$ mit $r = p(a)$. Mit eukl. Alg. ex. $q, r_1 \in K[X]$ mit $\mathrm{grad}(r_1) < \mathrm{grad}(f)$ und $p = q \cdot f + r_1$.
- Also gilt: $r = p(a) = q(a) \cdot \underbrace{f(a)}_{=0} + r_1(a) = r_1(a)$.

  D.h. $r = r_1(a) = \lambda_0 + \lambda_1 \cdot a + \ldots + \lambda_m a^m$

  mit $m = \mathrm{grad}(r_1) < \mathrm{grad}(f) = n$; insbes. $m \leq n-1$.

(ii) $1, a^1, \ldots, a^{n-1}$ sind lin. unabh.:

- Sei $\lambda_0 + \lambda_1 a^1 + \ldots + \lambda_{n-1} a^{n-1} = 0$ mit $\lambda_i \in K$.
- Für $p = \lambda_0 + \lambda_1 X + \ldots + \lambda_{n-1} X^{n-1} \in K[X]$ ist dann $p(a) = 0$. D.h. $p \in \ker(\varphi_a) = (f) = \{g \cdot f : g \in K[X]\}$.
- Ist $p \neq 0$, so ist $\mathrm{grad}(p) \geq \mathrm{grad}(f) = n$.
- Weil aber $\mathrm{grad}(p) = n-1 < n$ gilt $p = 0$, d.h. $\lambda_i = 0$ (für $0 \leq i \leq n-1$) und $1, a^1, \ldots, a^{n-1}$ sind lin. unabh.

$\dashv$

<u>Satz 14.4</u> Seien K, K' Körper und $\varphi : K \to K'$ ein Körperisomorphismus. Seien $L : K$, $L' : K'$ Körpererweiterungen, $a \in L$, $a' \in L'$, wobei gilt:

entweder (a) a ist transzendent über K und

a' ——— " ——— K',

oder (b) es ex. ein <u>irred.</u> Polynom $f \in K[X]$ mit $f(a) = 0$ und $(\varphi f)(a') = 0$.

Dann gilt: Es ex. ein Isom. $\tilde{\varphi} : K(a) \xrightarrow{\sim} K'(a')$ mit $\tilde{\varphi}(a) = a'$ und $\tilde{\varphi}|_K = \varphi$.

<u>Bem.</u> Adjungieren wir zwei versch. Nullstellen a, b eines irred. Polynoms $f \in K[X]$ zu K, so sind die erw. Körper $K(a)$ und $K(b)$ isom.

Beweis: Der Isom. $\varphi: K \xrightarrow{\sim} K'$ lässt erweitern zu einem Isom. $\varphi: K[X] \xrightarrow{\sim} K'[X]$, dieser lässt sich heben zu $\varphi: K(X) \xrightarrow{\sim} K'(X)$, wobei $K(X) = \mathrm{Quot}(K[X])$.

zu (a): Mit Satz 14.2 ist $K(a) \cong K(X)$, $K'(a') \cong K'(X)$, also $K(a) \cong K(X) \xrightarrow{\sim} K'(X) \cong K'(a')$.

zu (b): OBdA sei f normiert, also Minimalpolynom von a. Dann ist auch φf normiert und irred., also ist φf Minimalpolynom von a'.

- $K \xrightarrow[\varphi]{\sim} K' \hookrightarrow K'[a'] = K'(a')$ lässt sich heben zu

$$\begin{tikzcd} K[X] \arrow[r, "\sim"] \arrow[rrr, bend right, "\bar\varphi"'] & K'[X] \arrow[r, two heads, "\text{surj.}", "\text{Homom.}"'] & K'[X]/(\varphi f) \arrow[r, phantom, "\cong"] & K'[a'] = K'(a) \end{tikzcd}$$

$\bar\varphi$ surj. Homom. mit $\bar\varphi|_K = \varphi$ und $\bar\varphi(X) = a'$. (universelle Eigenschaft 12.3)

- $K[X]/\ker(\bar\varphi) \cong K'[X]/(\varphi f)$ (Folgerung aus Lem. 10.5)
- $\ker(\bar\varphi) = \{p \in K[X] : (\varphi p)(a') = 0\} = (f)$ (weil f irred. und (f) maximal)
- Somit gilt: $K(a) \overset{14.3}{\cong} \underbrace{K[X]/(f)}_{\text{weil } \ker(\bar\varphi) = (f)} \overset{\text{Folg.}}{\cong} K'[X]/(\varphi f) \overset{14.3}{\cong} K'(a')$.

$\dashv$

Folgerung 14.5 Sind $L:K$ und $M:K$ Körpererweiterungen, $a \in L$, $b \in M$ beide alg. über K, dann gilt:

a, b besitzen dasselbe Minimalpolynom

$\iff$ es ex. Isom. $\varphi: K(a) \xrightarrow{\sim} K(b)$ mit $\varphi(a) = b$ und $\varphi|_K = \mathrm{id}$.

Beweis: Übung.

Satz 14.6 Sei K ein Körper und $f \in K[X]$ mit $\text{grad}(f) = n \geq 1$. Dann ex. eine einfache Erweiterung $L = K(a)$ von K mit:

(a) a ist Nullstelle von f.

(b) $[K(a):K] \leq n$; $[K(a):K] = n$ gdw. f ist irred.

(c) Ist f irred., so ist L eindeutig bis auf Isomorphien welche eingeschränkt auf K die Identität sind.

Beweis: (c) folgt aus Folgerung 14.5.

Fall I f ist irreduzibel.

- Dann ist (f) max. Ideal und $K[X]/(f)$ ist ein Körper.
- Sei
$$\pi : K[X] \longrightarrow K[X]/(f) =: L$$
$$X \longmapsto \bar{X} =: a$$
(Adjunktion einer symbolischen Nullstelle)
- $\bar{X} = X + (f)$ nach Definition.

$a_n \bar{X}^n = a_n (X + (f))^n = a_n X^n + (f)$, und somit ist für $f = a_0 + a_1 X + \ldots + a_n X^n$: $f(\bar{X}) = a_0 + a_1 \bar{X} + \ldots + a_n \bar{X}^n =$
$$a_0 + a_1 X + (f) + \ldots + a_n X^n + (f) =$$
$$\underbrace{a_0 + a_1 X + \ldots + a_n X^n}_{=f} + (f) = (f) = 0 \in L.$$

D.h. $f(\bar{X}) = f(a) = 0$.

- $K \cong \pi[K] \subseteq L$ und a ist alg. über K.
- Ist nun, ohne Einschränkung, f normiert, so ist f Minimalpolynom von a über K.
- Also ist $[K(a):K] = n$ $(= \text{grad } f)$.

Fall II Ist f zerlegbar, so ist $f = \varepsilon \cdot f_1 \cdots f_r$ mit $\varepsilon \in K$ und f_i irred. über K.

- Mit Fall I ex. einfache Erweiterung $K(a)$ von K mit $f_1(a) = 0$ und $[K(a):K] = \text{grad}(f_1) < \text{grad}(f) = n$.

Satz 14.7 Sei $L:K$ eine Körpererweiterung, $A \subseteq L$ mit $L = K(A)$ und jedes Element aus A sei alg. über K.
Dann gilt: (a) $L:K$ ist algebraisch
(b) $|A| < \infty \implies [L:K] < \infty$

$L:K$ alg. & $L = K(A)$ für A endl. $\Leftarrow [L:K] < \infty$ (Übung)

Beweis: Wir zeigen (a) & (b) zusammen:

- Ist $r \in K(A)$, so ist $r = \frac{r_1}{r_2}$ für $r_1, r_2 \in K[A]$, weil $K(A) = \mathrm{Quot}(K[A])$.
- $K[A]$ besteht aus Polynomen der Form $\sum_{i=1}^{n} \lambda_i \alpha_i$ mit $\lambda_i \in K$ und $\alpha_i = a_{i_1}^{m_1} \cdot \ldots \cdot a_{i_k}^{m_k}$ mit $k \in \mathbb{N}$, $a_{i_\ell} \in A$, $m_\ell \in \mathbb{N}$ für $1 \le \ell \le k$.
- Somit ist $r = \frac{r_1}{r_2}$ mit $r_1, r_2 \in K[B]$ für eine endliche Menge $B \subseteq A$, d.h. $r \in K(B) = K(a_1, \ldots, a_n)$ wobei $B = \{a_1, \ldots, a_n\}$.
- Sei nun $B = \{a_1, \ldots, a_n\}$; $r \in K(a_1, \ldots, a_n) = K(B)$.
Für jedes $r \in K(A)$ ex. ein endl. $B \subseteq A$ mit $r \in K(B)$.
- Es gilt $K(a_1) \subseteq K(a_1, a_2) \subseteq \ldots \subseteq K(a_1, \ldots, a_n)$, und $K(a_1, \ldots, a_{i-1})(a_i) = K(a_1, \ldots, a_i)$.
- Für $a_i \in A$ ist nach Voraussetzung a_i alg. über K und somit ist a_i auch alg. über $K(a_1, \ldots, a_{i-1})$.
- Mit dem Gradsatz 14.1 ist dann $[K(B):K]$ endlich und mit Übungsaufgabe ist die Körpererw. $K(B):K$ alg.
- Somit ist $r \in K(B)$ alg. über K und weil r beliebig war, ist $K(A):K$ alg. (zu jedem $r \in K(A)$ ex. $B \subseteq A$, B endl.).

$\dashv$

Korollar 14.8 Sind $M:L$ und $L:K$ alg., so ist auch $M:K$ alg.

[siehe Übungen, auch für Umkehrung]

Satz 14.9 Sei $M:K$ eine Körpererweiterung und sei $L := \{a \in M : a \text{ alg. über } K\}$, so ist L ein Körper.

<u>Beweis:</u> $K \subseteq L \subseteq M$; seien $a, b \in M$ alg. über K.

z. zeigen: $a-b$, ab^{-1} (für $b \neq 0$) sind in L.

- Es gilt $K = K(a,b) \subseteq L$ und mit Satz 14.7.(a) ist $K(a,b) : K$ algebraisch.

Somit sind $a-b$ und ab^{-1} $(b \neq 0)$ alg. über K (weil sie in $K(a,b)$ liegen), also $a-b, ab^{-1} \in L$. ⊣

15. Zerfällungskörper

[Zuerst beweisen wir eine Folgerung aus Satz 14.6.]

<u>Korollar 15.1</u> Es sei $f \in K[X]$ ein beliebiges Polynom vom Grad n. Dann existiert ein Erweiterungskörper L von K mit $[L:K] \leq n!$, über dem f in Linearfaktoren zerfällt.

<u>Beweis:</u> Mit Induktion über n. Für $n=1$ ist f bereits in der richtigen Form. Sei $n \geq 2$ und sei die Aussage für alle $n' < n$ bewiesen. Mit Satz 14.6 ex. eine einfache Körpererweiterung $K(a) =: K_1$ mit $f(a) = 0$ und $[K_1 : K] \leq n$, da das Min. Pol. von a das Polynom f teilt.

- In K_1 gilt $f = (X-a) \cdot g$, wobei $g \in K_1[X]$ und $\text{grad}(g) = n-1 < n$.
- Nach Ind.-Vor. ex. $L \supseteq K_1$ über dem g in Linearfaktoren zerfällt. Dann zerfällt f in L in Linearfaktoren und weil mit Ind.-Vor. $[L : K_1] \leq (n-1)!$ ist, erhalten wir $[L:K] \leq n \cdot (n-1)! = n!$ ⊣

<u>Def.</u> Es sei $f \in K[X]$ gegeben. Der Oberkörper $L \supseteq K$ von minimalem Grad über K, über dem f in Linearfaktoren zerfällt, heisst <u>Zerfällungskörper</u> von f über K.