# Körpererweiterungen

Körpererweiterung $K \subseteq L$ (oft: $L/K$): $K \subseteq L$ Körper
$\leadsto L$ ist $K$-VR. $\boxed{\text{Grad}}$: $[L:K] := \dim_K(L)$

$\alpha \in L$ algebraisch über $K$: $\exists\, 0 \neq f \in K[X]: f(\alpha) = 0$

transzendent über $K$: sonst

$K \subseteq L$ algebraisch: alle $\alpha \in L$ algebr. über $K$

Bsp: $\mathbb{Q} \subseteq \mathbb{C}$ Körpererweiterung mit
- $\sqrt{2}$ algebraisch über $\mathbb{Q}$ $\quad (X^2-2)$
- $i$ algebraisch über $\mathbb{Q}$ $\quad (X^2+1)$
- $\pi$ transzendent über $\mathbb{Q}$ (o.B.)
- „f.a." Elemente sind transzendent (nur abz.bar viele sind algebraisch)

Bsp: $\underset{\text{Quot}(\mathbb{Q}[X])}{X}$ transzendent über $\mathbb{Q}$!

Al: Jeder Körper enthält ~~eine Kopie von $\mathbb{Q}$ oder $\mathbb{F}_p$ ($p$ prim)~~ ~~einen kleinsten Teilkörper~~ einen kleinsten Teilkörper, und dieser ist eine Kopie von $\mathbb{Q}$ oder $\mathbb{F}_p$ ($p$ prim).

Bew: klar, $\bigcap_{\substack{F \subseteq K \\ \text{Körper}}} F$ tut es. Wie sieht das aus? 0, 1 drin...

$\leadsto$ betrachte $\Phi: \mathbb{Z} \longrightarrow K,\ n \longmapsto n \cdot 1$

Erinnerung: $\ker(\Phi) = \langle \operatorname{char}(K) \rangle$

1. Fall: $\operatorname{char}(K) = p \leadsto \mathbb{F}_p \cong \operatorname{im}(\Phi) \subseteq K$ ✓

2. Fall: $\operatorname{char}(K) = 0 \leadsto \mathbb{Z} \cong \operatorname{im}(\Phi) \subseteq K$

$\overset{\text{rechnen}}{\leadsto} \mathbb{Q} \cong \{(n \cdot 1)(m \cdot 1)^{-1} : n, m \in \mathbb{Z}, m \neq 0\} \subseteq K$ ✓ $\square$

Dieser Körper heißt <u>Primkörper</u>.

**A2**: Bestimme <u>den</u> Körper der Ordnung 4 (falls es existiert) und zeige dass er algebraisch über seinem Primkörper ist.

**Lsg**: ~~(a) $\#K = 2^2 \leq 3$ ... $\alpha^4 - \alpha = 0$ für alle $\alpha \in K$~~

$\Rightarrow$

(1) $\#K = 4$

$\left.\begin{array}{l} \operatorname{char}(K) \mid \#K, \\ \text{prim} \end{array}\right\} \Rightarrow \operatorname{char}(K) = 2$ ~~$\Rightarrow$ Primkörper $\cong \mathbb{F}_2$~~

$\Rightarrow \underset{2}{\mathbb{F}_2} \subseteq \underset{2^{(2)}}{K}$ und $\dim_{\mathbb{F}_2}(K) = 2$

$\Rightarrow (K,+) \cong \mathbb{F}_2 \times \mathbb{F}_2$ (als $\mathbb{F}_2$-VR) und $(\underset{3}{K^\times}, \cdot) \cong \mathbb{F}_3$

~~$= \{(0,0), (0,1), (1,0), (1,1)\}$~~

Ansatz: ~~wähle $a \in K \setminus \{0,1\}$~~

$K =: \{0, 1, a, b\}$

$\rightsquigarrow$

| + | 0 | 1 | a | b |
|---|---|---|---|---|
| 0 | 0 | 1 | a | b |
| 1 | 1 | 0 | b | a |
| a | a | b | 0 | 1 |
| b | b | a | 1 | 0 |

$\mathbb{F}_2 \times \mathbb{F}_2$

| · | 0 | 1 | a | b |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | a | b |
| a | 0 | a | b | 1 |
| b | 0 | b | 1 | a |

$\mathbb{F}_3$

(2) $\#K^\times = 3 \Rightarrow \alpha^3 = 1 \quad (\forall \alpha \in K^\times)$

$\Rightarrow \alpha^4 - \alpha = 0 \quad (\forall \alpha \in K) \Rightarrow$ Poly $X^4 - X \in \mathbb{F}_2[X]$ tut es. $\square$

$K \subseteq L$ Körpererweiterung, $\alpha \in L$

$$K(\alpha) := \bigcap_{\substack{M \subseteq L \text{ Körper} \\ K \cup \{\alpha\} \subseteq M}} M$$

Adjunktion von $\alpha$ zu $K$, kleinster Teilkörper ~~Körper~~ von $L$, der $K$ und $\alpha$ enthält

Erinnerung:

$$K[\alpha] = \bigcap_{\substack{M \subseteq L \text{ Ring} \\ K \cup \{\alpha\} \subseteq M}} M$$

kleinster Teilring von $L$, der $K$ und $\alpha$ enthält

$$= \{ f(\alpha) : f \in K[X] \} = \mathrm{im}(\Phi_\alpha)$$

mit

$$\Phi_\alpha : K[X] \longrightarrow L, \quad f \longmapsto f(\alpha)$$

A3: ~~Frage:~~ Wie sieht $K(\alpha)$ aus?

Lsg: klar: $\mathrm{im}(\Phi_\alpha) = K[\alpha] \subseteq K(\alpha) \Rightarrow \boxed{K(\alpha) = \mathrm{Quot}(K[\alpha])}$

1. Fall: $\alpha$ algebraisch:

$$\Rightarrow \ker(\Phi_\alpha) = \{ f \in K[X] : f(\alpha) = 0 \} \neq \{0\}$$

Verschwindungsideal: prim, $\neq \{0\} \Rightarrow$ maximal

HIR $\Rightarrow \ker(\Phi_\alpha) =: \underbrace{m_{\alpha,K}}_{\text{Minimalpolynom (falls normiert)}} K[X]$

$\Leftrightarrow$

$$\Rightarrow \underbrace{K[X] / m_{\alpha,K} K[X]}_{\text{Körper}} \cong K[\alpha]$$

$$\Rightarrow \boxed{K(\alpha) = K[\alpha]}, \quad [K(\alpha) : K] = \deg(m_{\alpha,K})$$

2. Fall: $\alpha$ transzendent: $\Phi_\alpha$ injektiv

~~ker $\Phi_\alpha$~~

$$\Rightarrow \underbrace{k[X]}_{\text{kein Körper}} \cong k[\alpha] \subsetneq k(\alpha)$$

$$\cancel{\Rightarrow k(X) := \mathrm{Quot}(k[X]) \cong k(\alpha)}$$

$$\Rightarrow \boxed{k(\alpha) \cong \mathrm{Quot}(k[X]) =: k(X)},$$

~~$\dim_k k(\alpha)$~~

$[k(\alpha):k] \geq \dim_k k[\alpha]$

$\cancel{\geq [k(X):k]}$

$\geq \dim_k k[X] = \infty$

Folgerung:

$\alpha$ algebraisch über $k$

$\Leftrightarrow k(\alpha) = k[\alpha]$

$\Leftrightarrow \dim_k k[\alpha] < \infty$

$\Leftrightarrow [k(\alpha):k] < \infty$

$\quad ( \overset{\|}{\deg(m_{\alpha,k})} )$

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

• $\mathbb{Q}(i) = \{a + ib : a, b \in \mathbb{Q}\}$

• $\mathbb{Q}[\pi] \neq \mathbb{Q}(\pi)$

Folg: $[L:k] < \infty \Rightarrow$ ~~$k(\alpha)$~~ $k \subseteq L$ algebraisch

$\not\Leftarrow$

$\uparrow \mathbb{Q} \subseteq \ldots \subseteq \mathbb{C}$

Prop: (i) $k \subseteq \{\alpha \in L : \alpha \text{ alg. über } k\} \subseteq L$ Körpererw.

(ii) $k \subseteq L$ alg., $L \subseteq M$ alg $\Rightarrow k \subseteq M$ alg.

(iii) $[M:k] = [M:L] \cdot [L:k]$

dazu

A4: $K \subseteq L \subseteq M$ Körpererw.

$$\left.\begin{array}{l} B \subseteq L \text{ K-Basis von } L \\ C \subseteq M \text{ L-Basis von } M \end{array}\right\} \Rightarrow \underset{(\subseteq M)}{BC} \text{ K-Basis von } M$$

Bew: (1) EZS: $x \in M$

$$\Rightarrow \exists (\lambda_c) \subseteq L: \quad x = \sum_{c \in C} \lambda_c \cdot c$$

$$\Rightarrow \forall c\ \exists (\lambda_{b,c}) \subseteq K: \quad c = \sum_{b \in B} \lambda_{b,c} \cdot b$$

$$\Rightarrow x = \sum_{b,c} \lambda_{b,c} \cdot b \cdot c$$

(2) l.u.:

$$\sum_{b,c} \lambda_{b,c} \cdot b \cdot c = 0, \quad (\lambda_{b,c}) \subseteq K$$

$$\|$$

$$\sum_c \underbrace{\left( \sum_b \lambda_{b,c} \cdot b \right)}_{\in L} \cdot c = 0$$

$$\Rightarrow \forall c \in C: \quad \sum_b \underbrace{\lambda_{b,c}}_{\in K} \cdot b = 0$$

$\Rightarrow$ ~~[illegible]~~ $\lambda_{b,c} = 0 \quad (\forall b, c)$. $\square$

# Algebraischer Abschluss

Prop: $f \in k[X]$ normiert

$\Rightarrow \exists$ Körper $L \supseteq k$: $f$ zerfällt in Linearfaktoren, ~~Zerfällungskörper~~

$[L:k] \leq \deg(f)$!

Idee: Induktion über $\deg(f)$

IS: $f$ nicht irred. ~~hat NST~~ $\Rightarrow$ abspalten, IH

$f$ irred. $\Rightarrow$ $\underbrace{k[X]/fk[X]}_{=:L}$ Körper, der $k$ enthält, $[L:k] = \deg(f)$

und $\bar{X}$ ist NST von $f$ in $L$, da

$$f(\bar{X}) = \overline{f(X)} = \bar{f} = \bar{0}$$

$\rightsquigarrow$ abspalten, IH. $\square$

---

$k$ algebraisch abgeschlossen: es gibt keinen echten algebr. Erweiterungskörper

$\Leftrightarrow$ jedes nichtkonst. Polynom hat NST

$\Leftrightarrow$ jedes normierte Polynom zerfällt in LFen

$\rightsquigarrow$ $\mathbb{C}$ ist algebr. abgeschlossen, $\mathbb{R}$ und $\mathbb{Q}$ nicht.

Algebraischer Abschluss von $k$: Algebr. Erw. $L \supseteq k$, die algebr. abg. ist

$\rightsquigarrow$ $\mathbb{C}$ algebr. Abschluss von $\mathbb{R}$, aber nicht von $\mathbb{Q}$

Satz: Für jeden Körper existiert ein algebr. Abschluss $\bar{k}$.

(eind. bis auf Iso)

~~A5: Jedes Polynom $0 \neq f \in k[X] \Rightarrow f$ hat höchstens $\deg(f)$ NSTen~~

~~Bew:~~

~~$f \sim e \cdot f_{nor}$~~

~~$\Rightarrow \alpha$ NST von $f \Leftrightarrow \alpha$ NST von $f_{nor}$~~

~~und~~

~~Bew: Induktion.~~

- ~~$\deg(f) = 0$ ✓~~
- ~~$\deg(f) > 0$:~~

A5: Jedes Polynom $0 \neq f \in k[X]$ hat höchstens $\deg(f)$ NSTen

Bew: NSTen in $k \subseteq$ NSTen in $\overline{k}$

und in $\overline{k}$:

$$f = \underset{\substack{\cap \\ k^{\times}}}{e} \cdot \underbrace{(X - a_1) \cdots (X - a_d)}_{\text{irreduzibel, eind. bis auf Reihenfolge und Einheiten}} \leftarrow \text{wegen Grad}$$

$\Rightarrow \leq d$ NSTen

~~A6: $k$ endlich $\Rightarrow k$ nicht algebr. abg.~~

~~Bew: Zeige: Es gibt irred. Polynome beliebig größer Ordnung!~~

~~Bekannt: $\{X, \dots, X-(p-1)\}$ irred., $p = \mathrm{char}(k) > 1$~~

~~und~~

~~$f \in k[X]$ irred $\Rightarrow \{f \cdot g - 1\}$ irred~~

$\# k < \infty$

~~$\rightsquigarrow$ Zeige: Es gibt unendlich viele irred. Polynome~~ Ann: endl.

$\rightsquigarrow$ Idee: $M := \{f : f \text{ irred}\} \ni \{X, \dots, X-(p-1)\} \neq \emptyset \Rightarrow$ $\Rightarrow$

<u>A6</u>: $k$ endl. $\Rightarrow$ $k$ <u>nicht</u> alg. abg.

~~Bew: Betrachte~~

~~$k :=$~~

~~Bew: $k$ alg. abg. $\Rightarrow$ nur $(x-a)$~~

<u>Bew</u>: $k$ algebr. abg.

$\Rightarrow$ nur $\{(x-a) : a \in k\}$ irreduzibel

Betrachte

$$\left(\prod_{a \in k} x-a\right)+1 =: f$$

~~$\Rightarrow$ Grad $> 1$~~

$\Rightarrow \deg(f) > 1$, $f(b) = 1$ $(\forall b \in k)$ $\lightning$ $\square$

~~$f$ red. (sonst $1 \in (x-a_0)$)~~

# Irreduzibilität

**Kriterium von Eisenstein:** $R$ kommut, nullteilerfrei, $P \subseteq R$ Primideal,

$$\left.\begin{array}{l} f = \sum_{i=0}^{d} a_i X^i \in R[X] \\ a_0, \dots, a_{d-1} \in P \\ a_d \notin P \\ a_0 \notin P \cdot P \end{array}\right\} \Rightarrow f \text{ nicht Produkt zweier Polynome in } R[X] \text{ kleineren Grades}$$

~~("f nicht zerlegbar in R[X]")~~

($\neq$ irreduzibel z.B. in $\mathbb{Z}[X]$, also für R nicht Körper)

**Prop:** $R$ Hauptidealring, $K = \mathrm{Quot}(R)$.

$$\left.\begin{array}{l} f \in R[X] \\ f \text{ nicht Produkt zweier} \\ \text{Polynome in } R[X] \text{ kleineren Grades} \end{array}\right\} \Rightarrow f \text{ irreduzibel in } K[X]$$

**Bsp:** $X^n - p$ irreduzibel in $\mathbb{Q}[X]$ ~~für~~ ($p$ prim)

**A7:** ~~Bestimme~~ Finde alg. Körpererweiterung von unendl. Grad über $\mathbb{Q}$.

**Lsg:**

$$\left.\begin{array}{l} \sqrt[n]{2} \text{ NST von } X^n - 2 \\ X^n - 2 \text{ irred., normiert in } \mathbb{Q}[X] \\ \deg(X^n - 2) = n \end{array}\right\} \Rightarrow [\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$$

und

$$\mathbb{Q}(\sqrt[n]{2}) \subseteq \mathbb{Q}(\sqrt[2n]{2})$$

$$\Rightarrow K := \bigcup_{k \in \mathbb{N}} \mathbb{Q}(\sqrt[kn]{2})$$

ist Körper, alg. über $\mathbb{Q}$, Grad $\infty$! $\square$

A8: Sei $\rho := e^{2\pi i/7} = \cos(2\pi/7) + i\cdot\sin(2\pi/7)$. Bestimme

MP von $\rho$ und $[\mathbb{Q}(\rho):\mathbb{Q}]$

~~Bew.~~

Lsg: (1) $\rho$ ist NST von $\cancel{\in} X^7 - 1 = (X-1)\underbrace{(1+X+\dots+X^6)}_{=:m}$

$\Rightarrow m(\rho) = 0$.

$\Rightarrow [\mathbb{Q}(\rho):\mathbb{Q}] \leq 6$

(2) Idee: Betrachte $\tau := \rho + \rho^6$ denn $\mathbb{Q} \subseteq \mathbb{Q}(\tau) \subseteq \mathbb{Q}(\rho)$

$\Rightarrow \tau^2 = \rho^2 + \rho^5 + 2$

$\Rightarrow \tau^3 = \rho^3 + 3\rho + 3\rho^6 + \rho^4$

$\Rightarrow \tau$ ist NSTe von $\underbrace{X^3 + X^2 - 2X - 1}$

irreduzibel, denn sonst

$= (X-a)(X^2 - bX - c)$ in $\mathbb{Z}[X]$

$\Rightarrow ac = -1$

$\Rightarrow$ hat NSTen in $\{\pm 1\}$ ↯

$\Rightarrow [\mathbb{Q}(\tau):\mathbb{Q}] = 3$

~~$\Rightarrow 3|$~~

(3) $[\mathbb{Q}(\rho):\mathbb{Q}] \leq 6$

$[\mathbb{Q}(\rho):\mathbb{Q}] > [\mathbb{Q}(\tau):\mathbb{Q}]$ denn $\mathbb{Q}(\tau) \subseteq \mathbb{R}$, $\mathbb{Q}(\rho) \not\subseteq \mathbb{R}$

~~$[\mathbb{Q}(\tau):\mathbb{Q}]$~~

$3 \mid [\mathbb{Q}(\rho):\mathbb{Q}]$

$\Rightarrow [\mathbb{Q}(\rho):\mathbb{Q}] = 6$ und $m$ MP.

□