## Erinnerung:

Der *Grad* einer Körpererweiterung $L/K$ ist die Zahl

$$[L/K] \;:=\; \dim_K(L) \;\in\; \mathbb{Z}^{\geqslant 1} \cup \{\infty\}.$$

**3.2.4 Proposition:** Für jeden Körperturm $M/L/K$ gilt

$$[M/K] \;=\; [M/L]\cdot[L/K].$$

Insbesondere ist $M/K$ endlich genau dann, wenn $M/L$ und $L/K$ endlich sind.

**3.2.5 Proposition:** Jede endliche Körpererweiterung $L/K$ vom Primzahlgrad ist einfach, und für jedes $a \in L \smallsetminus K$ gilt $L = K(a)$.

$2 \neq 0$ in $K$.

---

**3.2.6 Proposition:** Für jede Körpererweiterung $L/K$ vom Grad 2 mit $\mathrm{char}(K) \neq 2$ existiert ein $a \in L$ mit $L = K(a)$ und $b := a^2 \in K$. Wir können dieses $a$ als *eine Quadratwurzel aus* $b$ ansehen.

Bew.: „Wähle $c \in L \smallsetminus K$. $\Rightarrow \{1, c\}$ Basis von $L$ über $K$. $\Rightarrow c^2 = \alpha c + \beta$ für gewisse $\alpha, \beta \in K$.

Setze $a := c - \frac{\alpha}{2} \Rightarrow a^2 = c^2 - \alpha c + \frac{\alpha^2}{4} = \beta + \frac{\alpha^2}{4} =: b \in K$.

$\Rightarrow a \in L \smallsetminus K$. $\Rightarrow L = K(a)$. ged.

**3.2.7 Vorsicht:** Die Notation $a = \sqrt{b}$ ist sehr gefährlich wegen fehlender Eindeutigkeit! Nur in $\mathbb{R}^{\geqslant 0}$ sind Wurzeln eindeutig definiert.

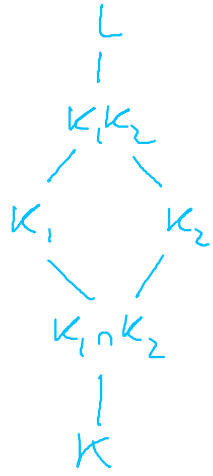
**3.2.8 Proposition:** Sei $L/K$ eine Körpererweiterung, und sei $R \subset L$ ein Unterring mit $K \subset R$ und $\dim_K(R) < \infty$. Dann ist $R$ ein Zwischenkörper.

Bsp.: $K = \mathbb{Q}$, $K_1 = \mathbb{Q}(x)$, $K_2 = \mathbb{R}$, $K_1 K_2 = \mathbb{R}(x)$

$\sum_{i=1}^{n} p_i(x) \cdot y_i$ ($p_i(x) \in \mathbb{Q}(x)$, $y_i \in \mathbb{R}$)

$\frac{1}{x - \pi}$ gilt nicht.

**3.2.9 Definition:** Für je zwei Zwischenkörper $K_1$ und $K_2$ einer Körpererweiterung $L/K$ bezeichnen wir den von $K_1 \cup K_2$ erzeugten Zwischenkörper mit $K_1 K_2$.




**3.2.10 Proposition:** In dieser Situation gilt, falls $K_1/K$ endlich ist,

$$K_1K_2 = \{ \textstyle\sum_i x_i y_i \mid x_i \in K_1,\ y_i \in K_2 \},$$
$$[K_1K_2/K_2] \leqslant [K_1/K] \quad \text{und}$$
$$[K_1K_2/K] \leqslant [K_1/K] \cdot [K_2/K].$$

Beweis: Sei $v_1, \dots, v_n$ eine Basis von $K_1$ über $K$.

$\Rightarrow R := \{ \sum_{i=1}^{n} v_i y_i \mid y_i \in K_2 \}$ ist $K_2$-Unterraum. $K_1$ $K_2$

$\forall i,j$, $v_i v_j \in K_1$ Reihe $\left(\sum_i v_i y_i\right) \cdot \left(\sum_j v_j y_i'\right) = \sum_{i,j} v_i v_j y_i y_j' \in R$.

$\Rightarrow R$ Unterring mit $K_2 \subset R$.

$\dim_{K_2} R < \infty \overset{3.2.8}{\Rightarrow} R$ Körper mit $K_1 \cup K_2 \subset R \Rightarrow K_1K_2 \subset R \subset K_1K_2 \Rightarrow R = K_1K_2$.

$[K_1K_2/K_2] = \dim_{K_2}(R) \leq n = [K_1/K]$.

$[K_1K_2/K] = [K_1K_2/K_2] \cdot [K_2/K] \leq [K_1/K] \cdot [K_2/K]$.

qed.

**3.2.11 Definition:** Gilt $[K_1K_2/K] = [K_1/K]\cdot[K_2/K] < \infty$, so heissen $K_1$ und $K_2$ *linear disjunkt über $K$.*

**3.2.12 Vorsicht:** Dies impliziert $K_1 \cap K_2 = K$, ist aber nicht äquivalent dazu.

Bew.: Sei $K' := K_1 \cap K_2 \Rightarrow [K_1K_2/K] = [K_1K_2/K']\cdot[K'/K] \le [K_1/K']\cdot[K_2/K']\cdot[K'/K]$

$[K_1/K]\cdot[K_2/K]$ $\Rightarrow$ $[K_1/K] \le [K_1/K']$ $\Rightarrow [K'/K] \le 1 \Rightarrow K' = K$. qed

$= [K_1/K'][K'/K]$

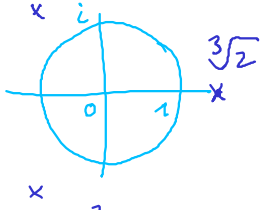
**3.2.13 Beispiel:** $\mathbb{Q}(i)$ und $\mathbb{Q}(\sqrt{2})$ sind quadratisch und linear disjunkt über $\mathbb{Q}$.

$\mathbb{Q}(i,\sqrt{2})$ — $=2$ / $\le 2$ nach 3.2.10 — $\mathbb{Q}(\sqrt{2})$ — $2$ — $\mathbb{Q}$

Wenn $\mathbb{Q}(\sqrt{2}) \subset \mathbb{R} \not\ni i$ ist $\mathbb{Q}(i,\sqrt{2}) \neq \mathbb{Q}(\sqrt{2})$

Hier ist $1, \sqrt{2}, i, \sqrt{2}\cdot i$ eine Basis von $K_1K_2$ über $K$.

**3.2.14 Beispiel:** $\mathbb{Q}(\sqrt[3]{2})$ und $\mathbb{Q}(\sqrt[3]{2}\,e^{2\pi i/3})$ sind vom Grad 3 und nicht linear disjunkt über $\mathbb{Q}$.




$L := \mathbb{Q}\left(\sqrt[3]{2}, \sqrt[3]{2}\cdot e^{\frac{2\pi i}{3}}\right) = \mathbb{Q}\left(\sqrt[3]{2}, e^{\frac{2\pi i}{3}}\right)$

$= \mathbb{Q}\left(\sqrt[3]{2}, \frac{-1+\sqrt{3}\cdot i}{2}\right)$

$= \mathbb{Q}\left(\sqrt[3]{2}, \sqrt{3}\cdot i\right)$

$\in \mathbb{R}$, also $\notin \mathbb{Q}(\sqrt[3]{2})$

aber $(\sqrt{3}i)^2 = -3 \in \mathbb{Q}$.

$X^3 - 2$ irreduzibel über $\mathbb{Q}$.

$\Rightarrow [L/\mathbb{Q}(\sqrt[3]{2})] = 2$.

$\Rightarrow [L/\mathbb{Q}] = [L/\mathbb{Q}(\sqrt[3]{2})]\cdot[\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}] = 2\cdot 3 < 3\cdot 3$.

$L$ — $2$ — $\mathbb{Q}(\sqrt[3]{2})$ — $3$ — $\mathbb{Q}$

$L$ — $2$ — $\mathbb{Q}(\sqrt[3]{2}\cdot e^{\frac{2\pi i}{3}})$ — $3$ — $\mathbb{Q}$

## 3.3 Einfache Körpererweiterungen

Betrachte eine Körpererweiterung $L/K$ und ein Element $a \in L$.

**3.3.1 Definition:** Existiert ein Polynom $f \in K[X] \setminus \{0\}$ mit $f(a) = 0$, so heisst $a$ *algebraisch über* $K$, andernfalls *transzendent über* $K$.

**3.3.2 Definition:** Eine komplexe Zahl heisst *algebraisch* bzw. *transzendent*, wenn sie algebraisch bzw. transzendent über $\mathbb{Q}$ ist.

**3.3.3 Beispiel:** Die Zahlen $i$ und $\sqrt{2}$ sind algebraisch.

$f = X^2 + 1$ $\qquad$ $f = X^4 - 4$

**3.3.4 Satz:** Die reellen Zahlen $e$ und $\pi$ sind transzendent. (ohne Beweis)

Betrachte nun den Auswertungshomomorphismus

$$\mathrm{eval}_a \colon K[X] \twoheadrightarrow K[a] \subset L, \ f \mapsto f(a).$$

**3.3.5 Proposition:** Es sind äquivalent:

(a) $a$ ist algebraisch über $K$.

(b) $\mathrm{Kern}(\mathrm{eval}_a) \neq (0)$.

(c) $\dim_K(K[a]) < \infty$.

(d) $[K(a)/K] < \infty$.

Bew.: (a) $\Leftrightarrow$ (b) gilt nach Def. 3.3.1.

Für $f \in K[X]$ vom Grad $n \geq 0$ ist $\dim_K (K[X]/(f)) = n$.
weil die Bilder von $1, X, \ldots, X^{n-1}$ eine Basis bilden.
wegen Division mit Rest durch $f$.

(b) $\Rightarrow$ Wähle $f \in \ker \setminus \{0\} \Rightarrow \dim K[X]/\ker(\mathrm{eval}_a)$
$\dim_K K[a]$ $\leq \dim_K K[X]/(f) < \infty \Rightarrow$ (c).

(c) $\Rightarrow$ $K[X] \twoheadrightarrow K[a]$ $\Rightarrow$ eval nicht injektiv $\Rightarrow$ (b).
$\dim = \infty$ $\dim < \infty$

**3.3.6 Proposition:** Es sind äquivalent:

(a) $a$ ist transzendent über $K$.

(b) $\mathrm{eval}_a$ ist injektiv.

(c) $\mathrm{eval}_a$ induziert einen Isomorphismus $K(X) \xrightarrow{\sim} K(a)$.

(d) $[K(a)/K] = \infty$.

(c) $\Rightarrow$ $K[a]$ Körper nach 3.2.8 $\Rightarrow K[a] = K(a) \Rightarrow$ (d)
(d) $\Rightarrow$ (c) wegen $K[a] \subset K(a)$ qed.

(a), (b), (d) sind die Negationen von
(a), (b), (d) aus 3.3.5.
Die sind äquivalent zur Isomorphie
$K[X] \xrightarrow{\sim} K[a]$.
$\Leftrightarrow$ $K(X) \xrightarrow{\sim} K(a) \Leftrightarrow$ (c). qed.

**3.3.7 Bemerkung:** Insbesondere sind $\mathbb{Q}(e)$ und $\mathbb{Q}(\pi)$ isomorph zu $\mathbb{Q}(X)$.

**3.3.8 Proposition:** Sei $a$ algebraisch über $K$. Dann gilt:

(a) $\mathrm{Kern}(\mathrm{eval}_a) = (m_a)$ für genau ein normiertes Polynom $m_a = m_{a,K} \in K[X]$.

(b) $m_a$ ist das eindeutige normierte Polynom von minimalem Grad in $\mathrm{Kern}(\mathrm{eval}_a)$.

(c) $m_a$ ist das eindeutige irreduzible normierte Polynom $f \in K[X]$ mit $f(a) = 0$.

(d) $\mathrm{eval}_a$ induziert einen Isomorphismus

$$K[X]/(m_a) \xrightarrow{\sim} K(a),\ f + (m_a) \mapsto f(a).$$

(e) $[K(a)/K] = \deg(m_a)$.

**3.3.9 Definition:** Das Polynom $m_a = m_{a,K}$ heisst das *Minimalpolynom von $a$ über $K$*. Sein Grad heisst auch der *Grad von $a$ über $K$*.

Bew.: $\mathfrak{a} := \mathrm{Kern}(\mathrm{eval}_a) \subset K[X]$ Ideal, $\neq (0)$.

Später: $\exists!\ m_a \in K[X]$ normiert mit $\mathfrak{a} = (m_a)$.

und dieses ist das eindeutige normierte Element von $\mathfrak{a}$ von kleinstem Grad.

Wähle $f \in \mathfrak{a} \setminus \{0\}$ von minimalem Grad.
$\forall g \in \mathfrak{a}$: Division mit Rest $\Rightarrow \exists\ h, l \in K[X]$:
$g = h \cdot f + l$ und $\deg(l) < \deg(f)$
$\Rightarrow l = g - hf \in \mathfrak{a} \longrightarrow \Rightarrow l = 0$.
Also ist $\mathfrak{a} = (f)$ | OBdA $f$ normiert.

Eindeutigkeit: Falls $\mathfrak{a} = (f) = (g)$ mit
$f, g$ normiert $\Rightarrow \deg(f-g) < \deg(f)$
$\Rightarrow f - g = 0$.

$\Rightarrow$ (a), (b).

Homomorphiesatz $\Rightarrow K[X]/(m_a) \xrightarrow{\sim} K[a] \simeq K(a)$

$\Rightarrow$ (d) $\Rightarrow$ (e)

$\dim = \deg(m_a)$

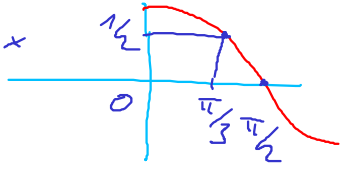
$K(a)$ Körper $\Rightarrow (m_a)$ max. Ideal $\Rightarrow m_a$ irred.
Sei $f$ normiert irred. mit $f(a) = 0 \Rightarrow f \in (m_a) \Rightarrow m_a \mid f \Rightarrow m_a = f$.
$\Rightarrow$ (c) gezeigt

**3.3.10 Beispiel:** Die reelle Zahl $\omega := \cos\frac{\pi}{9}$ ist algebraisch mit $m_{\omega,\mathbb{Q}}(X) = X^3 - \frac{3}{4}X - \frac{1}{8}$ und $[\mathbb{Q}(\omega)/\mathbb{Q}] = 3$.

$\cos 3x = \cos x \cdot \cos 2x - \sin x \cdot \sin 2x = \cos x(2\cos^2 x - 1) - \sin x \cdot 2\sin x \cos x$

$= 2\cos^3 x - \cos x - 2\cdot\cos x(1-\cos^2 x) = 4\cos^3 x - 3\cos x$

$\Rightarrow \cos\frac{\pi}{3} = 4\omega^3 - 3\omega = \frac{1}{2}$




**3.3.11 Bemerkung:** Im Fall $n := [K(a)/K] < \infty$ ist jedes Element von $K(a)$ gleich $f(a)$ für ein eindeutiges Polynom $f \in K[X]$ vom Grad $< n$. Die Summe zweier solcher Elemente berechnet sich direkt, das Produkt durch Division mit Rest als $f(a)g(a) = r(a)$ für $q, r \in K[X]$ mit $fg = qm_a + r$ und $\deg(r) < n$. Ist $f(a) \neq 0$, so gilt $\mathrm{ggT}(f, m_a) \sim 1$ in $K[X]$. Mit dem euklidischen Algorithmus findet man dann Polynome $u, v \in K[X]$ mit $uf + vm_a = 1$. Auswerten in $a$ liefert dann die Gleichung $u(a)f(a) = 1$, also $f(a)^{-1} = u(a)$.

**3.3.12 Beispiel:** Für $a := \sqrt[3]{2}$ ist $m_{a,\mathbb{Q}}(X) = X^3 - 2$ und $\frac{1}{1+a} = \frac{1-a+a^2}{3}$.