Erinnerung: Betrachte eine algebraische Körpererweiterung L/K.

(a) Ein Element von L, dessen Minimalpolynom über K separabel ist, heisst *separabel über* K.

(b) Ist jedes Element von L separabel über K, so heisst L/K *separabel.*

6.8.4 Proposition: Sei $L = K(a_1, \ldots, a_n)/K$ endlich, und sei $\overline{K}$ ein algebraischer Abschluss von K. Dann sind äquivalent:

(a) L/K ist separabel.

(b) Jedes a_i ist separabel über K.

(c) $|\operatorname{Hom}_K(L, \overline{K})| = [L/K]$. ($\leq$ gilt immer)

$$\begin{tikzcd} L \arrow[rr, dashed, "\psi"] & & \overline{K} \\ K(a) \arrow[u, dash] \arrow[urr, dashed, "\varphi"] & & \\ K \arrow[u, dash] \arrow[uurr, dash] & & \end{tikzcd}$$

Noch zu zeigen: (c) $\Rightarrow$ (a)

Sei $a \in L$ mit Minimalpolynom $f \in K[X]$ über K.

$\Rightarrow \quad \operatorname{Hom}_K(K(a), \overline{K}) \xrightarrow{\text{bij.}} \{ b \in \overline{K} \mid f(b) = 0 \} =: S$

$\qquad\qquad \varphi \longmapsto \varphi(a)$

$\Rightarrow \quad |\operatorname{Hom}_K(K(a), \overline{K})| = |S| \leq \deg(f) = [K(a)/K]$.

Für jedes φ gibt es $\leq [L/K(a)]$ Fortsetzungen in $\operatorname{Hom}_K(L, \overline{K})$.

$\Rightarrow \quad |\operatorname{Hom}_K(L, \overline{K})| = \sum_{\varphi} \#\text{Fortsetzungen} \leq [K(a)/K] \cdot [L/K(a)] = [L/K]$

$\qquad \| $

$\qquad [L/K]$

Gleichheit! $\Rightarrow |S| = \deg(f) \Rightarrow f$ separabel.

qed.

6.8.5 Proposition: Eine algebraische Körpererweiterung $L = K(A)/K$ ist separabel genau dann, wenn jedes Element von A separabel über K ist.

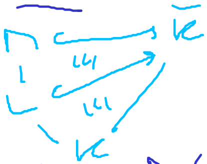
Beweis: "$\Rightarrow$" klar

"$\Leftarrow$" Jedes $b \in L$ ist in $\underbrace{K(a_1, \dots, a_n)}_{\text{separabel über } K \text{ nach } 6.8.4.}$ für gewisse $a_1, \dots, a_n \in A$.

$\Rightarrow$ b separabel über K. qed

6.8.6 Proposition: Für jeden algebraischen Körperturm $M/L/K$ ist M/K separabel genau dann, wenn M/L und L/K separabel sind.

Beweis: M/K separabel $\Rightarrow$ Jedes $a \in L$ ist auch in M $\Rightarrow$ separabel über K $\Rightarrow$ L/K separabel.



$\Rightarrow$ Sei $a \in M$ und $\left\{ \begin{array}{l} f \text{ sein Minpol über } K \\ g \text{ } \dots \dots \text{ } L \end{array} \right\}$ $\Rightarrow g \mid f$ in $L[X]$.

f separabel $\Rightarrow$ g separabel. $\Rightarrow$ a separabel über L $\Rightarrow$ M/L sep.

Sei nun M/L und L/K separabel.

Falls $[M/K] < \infty$ ist, folgt $|\mathrm{Hom}_K(M, \bar{K})| = \sum_{\underbrace{\varphi \in \mathrm{Hom}_K(L, \bar{K})}_{[L/K]}} \underbrace{\left| \{ \psi \in \mathrm{Hom}_K(M, \bar{K}) \mid \psi|_L = \varphi \} \right|}_{[M/L]}$

$= [L/K] \cdot [M/L] = [M/K]$. ✓

Allg. Fall: Sei $a \in M$ und $f := \sum_{i=0}^{d} b_i X^i$ sein Minpol. über L $\Rightarrow$ f separabel.

Setze $L' := K(b_0, \dots, b_d)$ | Dies ist auch das Minpol. von a über L'.

und $M' := L'(a)$

$\left. \begin{array}{l} \text{Dann ist } L'/K \text{ separabel.} \\ \text{und } M'/L' \text{ separabel.} \end{array} \right\}$ $\Rightarrow$ M'/K separabel. $\Rightarrow$ a separabel über K qed.

6.8.7 Satz vom primitiven Element: Jede endliche separable Körpererweiterung ist einfach.

Beweis: Induktion über $[L/K]$. Fall $L=K \Rightarrow L=K(a)$. Sonst sei L' ein max. Zwischenkörper $L' \neq L$. Dann ist $L' = K(a)$ und $L = L'(b)$ für jedes $b \in L \setminus L'$.

Also ist $L = K(a,b)$. Wähle Einbettung $L \hookrightarrow \overline{K}$. Sei $\left\{ \begin{array}{l} f \text{ das Min. Pol. von } a \text{ über } K \\ g \text{ --- --- --- } b \text{ ...} \end{array} \right\}$

Schreibe $\boxed{f(X) = \prod_{i=1}^{m} (X - a_i)}$ und $g(X) = \prod_{j=1}^{n} (X - b_j)$ mit $a_1 = a$ und $b_1 = b$.

Dann sind $a_1, \ldots, a_m$ bzw. $b_1, \ldots, b_n$ paarweise verschieden.

Beh 1: Ist $|K| = \infty$, so existiert $u \in K^\times$ so dass die $m \cdot n$ Elemente $a_i + u b_j \in \overline{K}$ paarweise verschieden sind.

Bew.: Für jedes $u \in K^\times$ und (i,j) und (i',j') gilt $\boxed{a_i + u b_j = a_{i'} + u b_{j'}} \Longleftrightarrow$

$$\left\{ \begin{array}{l} i = i' \text{ und } b_j = b_{j'} \Longleftrightarrow (i,j) = (i',j'). \\ \text{oder} \\ j = j' \text{ und } a_i = a_{i'} \Longleftrightarrow (i,j) = (i',j') \\ \text{oder} \\ i \neq i' \wedge j \neq j' \text{ und } a_i - a_{i'} = u \cdot (b_{j'} - b_j) \end{array} \right.$$

$$\Longleftrightarrow u = \frac{a_i - a_{i'}}{b_{j'} - b_j}.$$

Dies gilt nur für endlich viele $u \in K$!

Wegen $|K| = \infty$ ... qed.

Setze $c := a + ub = a_1 + u b_1$

Beh.: $L = K(c)$.

Bew.: Setze $h(X) := f(c - uX) \in K(c)[X]$.

Für alle $y \in \overline{K}$ gilt $h(y) = 0 \iff f(c-uy) = 0 \iff \exists i: c - uy = a_i$

$$\iff a_1 + ub_1 - uy = a_i \iff u(b_1 - y) = a_i - a_1 \iff y = b_1 + \frac{a_1 - a_i}{u}.$$

Insbesondere ist $y = b_1$ eine Nullstelle.

Nach Beh. 1 gilt $\frac{a_1 - a_i}{u} + b_1 = b_j \iff a_1 + ub_1 = a_i + ub_j \iff (i,j) = (1,1)$.

Also ist $y = b_1$ die einzige gemeinsame Nullstelle von h und g.

Da g separabel ist, ist der ggT von h und g in $\overline{K}[X]$ gleich $X - b$

Dies ist auch der ggT über $K(c)$. Also ist $b \in K(c)$

Damit folgt $a = c - ub \in K(c)$

$\Rightarrow K(a,b) = K(c)$.

qed.

Ist K endlich, ist L endlich $\Rightarrow L^\times$ zyklisch. Jeder Erzeuger a von $L^\times$ erfüllt $L = K(a)$.

qed.