Ad §5.13 : Separable Körpererweiterungen

Prop.: Sei $L = K(a_1, \dots, a_n)/K$ endlich, und sei $\bar{K}$ ein algebraisch Abschluss von K. Dann sind äquivalent:

(a) L/K separabel.

(b) Jedes a_i ist separabel über K.

(c) $|\mathrm{Hom}_K(L, \bar{K})| = [L/K]$.

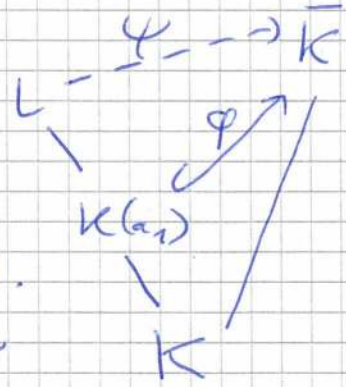
Beweis: (a) $\Rightarrow$ (b) klar (nach Def. von L/K separabel).

(b) $\Rightarrow$ (c) Induktion über n. Für $n=0$ sind beide Seiten $=1$.

Induktionsschritt $n-1 \rightsquigarrow n$: Wegen (b) ist das Minimalpolynom $m_{a_1,K}(X) \in K[X]$ separabel, hat also genau $\deg(m_{a_1,K}) = [K(a_1)/K]$ verschiedene Nullstellen in $\bar{K}$. Aus §5.7 folgt:

$$|\mathrm{Hom}_K(K(a_1), \bar{K})| = [K(a_1)/K].$$

Fixiere ein φ und Schwarze $\bar{K}$ via φ als Körpererweiterung von $K(a_1)$. Dann ist $\bar{K}$ ein algebraischer Abschluss von $K(a_1)$. Wir ordnen die möglichen Erweiterungen von φ zu einem Homo $\psi \in \mathrm{Hom}_K(L, \bar{K})$:



Für jedes $1 \le i \le n$ schwarze das Minimalpolynom $m_{a_i,K} \in K[X]$. Folglich es in $K(a_1)[X]$. Einer dieser Faktoren hat die Nullstelle a_i, und ist folglich gleich $m_{a_i,K(a_1)}$.

Da $m_{a_i,K}$ separabel ist, ist auch dieser Faktor separabel! Also ist jedes a_i separabel über $K(a_1)$.

Folglich erfüllt $L = K(a_1)(a_2, \dots, a_n)/K(a_1)$ die selben Bedingungen der Proposition, diesmal ist $n-1$ anstatt n. Somit besitzt φ genau $[L/K(a_1)]$ verschiedene Fortsetzungen ψ.

Insgesamt folgt

$$|\mathrm{Hom}_K(L, \bar{K})| = \sum_{\varphi} [L/K(a_1)] =$$

$$= [K(a_1)/K] \cdot [L/K(a_1)] = [L/K].$$

(c) $\Rightarrow$ (a) Sei $a \in L$ beliebig und $f \in K[X]$ ein Minimalpolynom über K. Nach §5.7 gilt

$$|\mathrm{Hom}_K(K(a), \bar{K})| = |\{a' \in \bar{K} \mid f(a') = 0\}| \leq \deg(f) = [K(a)/K].$$

Für jedes φ gilt ebenfalls nach §5.7

$$|\{\psi \in \mathrm{Hom}_K(L, \bar{K}) \mid \psi|_{K(a)} = \varphi\}| \leq [L/K(a)].$$

Zusammen liefert dies

$$|\mathrm{Hom}_K(L, \bar{K})| \leq [L/K(a)] \cdot [K(a)/K] = [L/K].$$

(Genau so funktioniert der Beweis in §5.7 !)

Nach (c) gilt hier aber Gleichheit. Also muss auch dort überall Gleichheit gelten. Daraus folgt f keine mehrfachen Nullstellen, ist also separabel. Somit ist a separabel über K. qed

Prop.: $L = K(A)/K$ ist separabel algebraisch genau dann, wenn jedes $a \in A$ separabel algebraisch über K ist.

Beweis: "$\Rightarrow$" klar nach Def.

"$\Leftarrow$": Jedes $a \in L$ liegt schon in $K(a_1, \ldots, a_n)$ für geeignete $a_1, \ldots, a_n \in L$. Nach (b) $\Rightarrow$ (a) des obigen Prop. ist folglich a separabel algebraisch über K. qed.

Satz vom primitiven Element: Jede endliche separable Körpererweiterung L/K ist einfach.

Beweis: Induktion nach $[L/K]$. Klar falls $[L/K]=1$.
Sonst wähle Zwischenkörper $K \subset L' \subsetneq L$ mit $[L'/K]$ maximal.
Für jedes $a \in L \setminus L'$ ist dann $L = L'(a)$. Nach Induktionsvoraussetzung ist andererseits $L' = K(b)$ für ein $b \in L'$.
Also folgt $L = K(a,b)$.

Wähle eine Einbettung von L in einen algebraischen Abschluss $\bar{K}$ von K. Sei f, g das Minimalpolynom von a, b über K.
Schreibe $f(X) = \prod_{i=1}^{m} (X - a_i)$ und $g(X) = \prod_{j=1}^{n} (X - b_j)$
mit $a_i, b_j \in \bar{K}$. Da a, b separabel über K sind, sind die $a_1, \dots, a_m$, respektive die $b_1, \dots, b_n$, paarweise verschieden.

Beh. 1: Ist $|K| = \infty$, so existiert $u \in K^\times$ so dass die $a_i + u b_j \in \bar{K}$ für alle (i,j) verschieden sind.

Beweis: Für jedes $u \in K^\times$ und je zwei Paare $(i,j) \neq (i',j')$ gilt $a_i + u b_j = a_{i'} + u b_{j'} \iff a_i - a_{i'} = u(b_{j'} - b_j)$.
Ist $j = j'$, so ist $b_{j'} - b_j = 0 \Rightarrow a_i - a_{i'} = 0 \Rightarrow i = i' \Rightarrow$ Widerspruch.
Also ist die äquivalent zu $\iff j \neq j' \wedge u = \frac{a_i - a_{i'}}{b_{j'} - b_j}$.
Da hier nur endlich viele Werte von u vermieden werden müssen, kann man so ein u finden, wenn $|K| = \infty$ ist. qed.

Wähle ein solches u und setze $c := a + bu$.

Beh. 2: $L = K(c)$.

Beweis: Betrachte das Polynom $h(X) := f(c - uX) \in K(c)[X]$.
Für alle $x \in \bar{K}$ gilt $h(x) = 0 \iff \exists i : c - ux = a_i$
$\iff \exists i : x = \frac{c - a_i}{u} = \frac{a - a_i}{u} + b$.
Insbesondere ist $x = b$ eine Nullstelle von h.
Nach Beh. 1 gilt $\forall i,j : \frac{a - a_i}{u} + b = b_j \iff a = a_i \wedge b_j = b$.
Also ist $x = b$ die einzige gemeinsame Nullstelle von h und g und zwar der Multiplizität 1.

Sei $k := \mathrm{ggT}(h, g) \in K(c)[X]$. Dann hat k also genau eine Nullstelle, und die mit Multiplizität 1, somit hat k den Grad 1, und seine Nullstelle b liegt in $K(c)$.

Also gilt $b \in K(c)$. Dann folgt dann $a = c - bu \in K(c)$ und somit $L = K(a,b) \subset K(c) \subset L \Rightarrow L = K(c)$. qed.

—

Dies beweist die Propositio im Falle $|K| = \infty$.
Für $|K| < \infty$ gilt auch $|L| < \infty$. Dann ist $L^\times$ zyklisch, z.B. $L^\times = \langle a \rangle$. Dann gilt offenbar $L = K(a)$. qed.

Beispiel: Sind $p_1, \dots, p_n$ paarweise verschiedene Primzahlen, und sind $a_1, \dots, a_n \in \mathbb{Q}$ so dass für alle Wahlen von Vorzeichen gilt $\pm a_1\sqrt{p_1} \pm \dots \pm a_n\sqrt{p_n}$ paarweise verschieden, so ist
$\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n}) = \mathbb{Q}(a_1\sqrt{p_1} + \dots + a_n\sqrt{p_n})$

Im Beispiel für $p_1 < \dots < p_n$ nimm $a_i = p_i$!