Algebra II, SoSe 2012 – Lösung Blatt 3

3.1. (i) Es bezeichne $f_\alpha(X) \in K[X]$ das Minimalpolynom von $\alpha \in E$ über K.

Nach Voraussetzung ist $\alpha^{p^e} \in K$, d.h. $X^{p^e} - \alpha^{p^e} \in K[X]$.

Da offenbar $\alpha \in E$ Nullstelle von $X^{p^e} - \alpha^{p^e}$ ist, folgt:

$$f_\alpha(X) \mid X^{p^e} - \alpha^{p^e}. \qquad (*)$$

Im algebraischen Abschluss $\overline{K}$ von K gilt (Frobenius!)

$$X^{p^e} - \alpha^{p^e} = (X-\alpha)^{p^e}$$

(beachte: $\alpha \in \overline{K}$). Da $X-\alpha$ irreduzibel ist, folgt also aus $(*)$:

$$f_\alpha(X) = (X-\alpha)^m \qquad (\text{in } \overline{K}!)$$

für ein $m \in \mathbb{N}$ mit $m \leq p^e$. Fallunterscheidung:

- falls $m = 1$, dann $f_\alpha(X) = X - \alpha = g(X^{p^0})$ für $g(X) = X - \alpha$
  d.h. $\deg g = \#\{\text{verschiedene Nullstellen von } f_\alpha \text{ in } \overline{K}\}$
- falls $m > 1$, dann besitzt f_α in $\overline{K}$ mehrfache Nullstellen
  $\overset{\text{VL}}{\underset{\text{char}(K)=p>0}{\Longrightarrow}}$ $\exists\, j \in \mathbb{N}$ und ein irreduzibles, separables Polynom $g(X) \in K[X]$ mit $f_\alpha(X) = g(X^{p^j})$ und $\deg g = \#\{\text{verschiedene Nullstellen von } f_\alpha \text{ in } \overline{K}\}$.

In jedem Fall erhalten wir also ein irreduzibles Polynom

$g \in K[X]$ mit $f_\alpha(X) = g(X^{p^j})$ für ein $j \in \mathbb{N}$ und

$$\deg g = \#\{\text{verschiedene Nullstellen von } f_\alpha \text{ in } \overline{K}\}.$$

Wegen $f_\alpha(X) = (X-\alpha)^m$ in $\overline{K}$ besitzt f_α aber nur eine „verschiedene" Nullstelle in $\overline{K}$ $\Rightarrow \deg g = 1$, d.h.

$$g(X) = X - a \quad \text{für ein } a \in K.$$

$$\Rightarrow f_\alpha(X) = g(X^{p^j}) = X^{p^j} - a.$$

Wegen $0 = f_\alpha(\alpha) = \alpha^{p^j} - a$ folgt $a = \alpha^{p^j}$, d.h.

$$f_\alpha(X) = X^{p^j} - \alpha^{p^j} = (X-\alpha)^{p^j} \quad \text{in } \overline{K}.$$

Also gilt $p^j = m \leq p^e$.

Da aber $\alpha^{p^j} = a \in K$ gilt, folgt wegen der Minimalität von e, dass $j \geq e$, also $p^j \geq p^e$ gelten muss.

$$\Rightarrow \quad m = p^j = p^e$$

und damit

$$f_\alpha(X) = X^{p^e} - \alpha^{p^e}.$$

(ii) • Sei $\alpha \in E$ separabel und rein inseparabel.

$f_\alpha(X) \in K[X]$ sei wieder das Minimalpolynom von α über K.

$\overset{(i)}{\Rightarrow}$ $f_\alpha(X) = X^{p^e} - \alpha^{p^e}$ für ein $e \in \mathbb{N} \cup \{0\}$.

In einem algebraischen Abschluss $\overline{K}$ von K gilt also:

$$f_\alpha(X) = X^{p^e} - \alpha^{p^e} = (X - \alpha)^{p^e}.$$

Da α separabel ist, besitzt f_α in $\overline{K}$ nur einfache Nullstellen.

$\Rightarrow p^e = 1$, d.h. $f_\alpha(X) = X - \alpha$

$\overset{f_\alpha \in K[X]}{\Rightarrow}$ $\alpha \in K$.

• Ist umgekehrt $\alpha \in K$, dann ist das Minimalpolynom von α über K offenbar $X - \alpha \in K[X]$, welches wegen $\deg(X - \alpha) = 1$ nur einfache Nullstellen besitzt.

$\Rightarrow \alpha$ ist separabel.

Da $\alpha^{p^0} = \alpha \in K$ gilt, ist α auch rein inseparabel.

3.2. Sei $\alpha \in E$ mit Minimalpolynom $f_\alpha(X) \in K[X]$ über K. Zu zeigen: f_α besitzt nur einfache Nullstellen.

Es gilt:

(*) f_α besitzt mehrfache Nullstellen $\Leftrightarrow \exists\, g \in K[X]$ mit $f_\alpha(X) = g(X^p)$

Denn:

Schreibe $f_\alpha(X) = \sum_{j=0}^{n} a_j X^j$. $\Rightarrow f_\alpha'(X) = \sum_{j=1}^{n} j \cdot a_j X^{j-1}$

Dann folgt:

f_α besitzt mehrfache Nullstellen

$\overset{\text{VL}}{\Leftrightarrow} f_\alpha' = 0 \Leftrightarrow j \cdot a_j = 0$ für $1 \leq j \leq n$

$\overset{\text{ch}(K)=p>0}{\Leftrightarrow} p \mid j$ oder $a_j = 0$ für $1 \leq j \leq n$.

$\Leftrightarrow$ Alle echt in f_α auftretenden Potenzen von X sind von der Form X^j mit $p \mid j$.

$\Leftrightarrow \exists\, g \in K[X]$ mit $f_\alpha(X) = g(X^p)$.

Damit ist (*) gezeigt.

$\nearrow$ f_α besitzt mehrfache Nullstellen.

$\overset{(*)}{\Rightarrow} f_\alpha(X) = g(X^p)$ für ein $g \in K[X]$.

$\Rightarrow \deg f_\alpha = p \cdot \deg g$

$\Rightarrow p \mid \deg f_\alpha$

Betrachte die einfache Erweiterung $K(\alpha)/K$. Da f_α Minimalpolynom von $\alpha \in E$ ist, folgt:

$$[K(\alpha) : K] = \deg f_\alpha$$

$$\Rightarrow \quad p \mid [K(\alpha) : K].$$

Da $K(\alpha) \subset E$ gilt, folgt aus dem Gradsatz

$$[E : K] = [E : K(\alpha)] \cdot [K(\alpha) : K]$$

und damit $p \mid [E : K]$ ↯ $p \nmid [E : K]$.

$\Rightarrow$ f_α besitzt nur einfache Nullstellen

$\Rightarrow$ $\alpha \in E$ separabel über K

$\overset{\alpha \in E \text{ bel.}}{\Rightarrow}$ E/K ist separabel.

∎

3.3. Erinnerung:

k vollkommen $\Leftrightarrow$ jedes irreduzible Polynom in $k[X]$ hat nur einfache Nullstellen

$\Leftrightarrow$ jede algebraische Erweiterung von k ist separabel.

(i) Sei L/E algebraische Erweiterung.

$\overset{E/K \text{ alg.}}{\Rightarrow}$ L/K ist algebraische Erweiterung

$\overset{K \text{ vollk.}}{\Rightarrow}$ L/K ist separable Erweiterung.

Wir zeigen, dass auch L/E separabel ist. Bemerkung:

L/E separabel $\Leftrightarrow$ jedes $\alpha \in L$ ist separabel über E

$\Leftrightarrow$ $\forall \alpha \in L$ besitzt das Minimalpolynom $f_\alpha \in E[X]$ nur einfache Nullstellen

(*)

$\Leftrightarrow$ jedes $\alpha \in L$ ist Nullstelle eines separablen Polynoms aus $E[X]$

Zur letzten Äquivalenz: „$\Rightarrow$" ist klar. „$\Leftarrow$": Ist α Nullstelle des separablen Polynoms $f \in E[X]$, dann folgt für das Minimalpolynom $f_\alpha \in E[X]$: $f_\alpha \mid f$. f_α muss also separabel sein, da sonst f nicht separabel wäre. ok.

Sei nun $\alpha \in L$ beliebig. L/K separabel $\overset{(*)}{\Rightarrow} \exists f \in K[X]$ separabel mit $f(\alpha) = 0$.

Dann ist aber auch $f \in E[X]$ separabel, d.h. α ist separabel über E (wegen (*)).

Da $\alpha \in L$ beliebig war, ist also L/E separabel.
Also ist jede algebraische Erweiterung von E separabel, d.h. E ist vollkommen.

(ii) Sei $f(X) \in K[X]$ irreduzibel.

Zu zeigen: f besitzt nur einfache Nullstellen.

OE sei f normiert (Einheiten ändern die Nullstellen nicht!)

Sei $\overline{K}$ algebraischer Abschluss von K mit $K \subset E \subset \overline{K}$ und $\alpha \in \overline{K}$ eine Nullstelle von f.

Sei $f_{\alpha,E} \in E[X]$ das Minimalpolynom von α über E (lese $f(X) \in E[X]$ ...).

Weiter sei E_1 der Körper, welcher über K von den Koeffizienten von $f_{\alpha,E}$ erzeugt wird, wir können also insbesondere auch $f_{\alpha,E} \in E_1[X]$ lesen.

Es genügt zu zeigen:

$$E_1(\alpha)/K \text{ ist separabel.} \qquad (*)$$

Denn ist (*) gezeigt, so folgt:
$f \in K[X]$ irreduzibel, normiert und $f(\alpha) = 0$

$\Rightarrow$ f ist das Minimalpolynom von α über K.

Mit (*): $E_1(\alpha)/K$ separabel $\overset{\text{insb.}}{\Rightarrow}$ α ist über K separabel

$\overset{f \text{ Minimal-polynom}}{\Rightarrow}$ f ist über K separabel, besitzt also nur einfache Nullstellen. ok.

Wir müssen also nur noch (*) zeigen. Dazu:

$f_{\alpha,E} \in E[X]$ irreduzibel und normiert

$\overset{\text{insb., da } E_1 \subset E}{\Rightarrow}$ $f_{\alpha,E} \in E_1[X]$ irreduzibel und normiert

$\Rightarrow$ $f_{\alpha,E} \in E_1[X]$ ist Minimalpolynom von α über E_1. (**)

Da E vollkommen und $f_{\alpha,E} \in E[X]$ irreduzibel ist, ist $f_{\alpha,E}$ separabel (auch als Polynom in $E_1[X]$).

$\overset{(**)}{\Rightarrow}$ α ist separabel über E_1

$\overset{\text{VL}}{\Rightarrow}$ $E_1(\alpha)/E_1$ ist separable Erweiterung.

Da nach Voraussetzung E/K separabel ist, und $K \subset E_1 \subset E$ gilt, ist nach Vorlesung auch E_1/K separabel, d.h.

$E_1(\alpha)/E_1$ und E_1/K sind separabel.

$\overset{\text{VL}}{\Rightarrow}$ $E_1(\alpha)/K$ ist separable Erweiterung.

Damit ist (*) nachgewiesen.

(iii) Wir konstruieren ein Gegenbeispiel:

Sei K ein Körper der Charakteristik $p > 0$.

- $K(Y) = \mathrm{Quot}(K[Y])$ ist Körper. ($K[Y]$: Polynomring in Y)

$K(Y)$ ist nicht vollkommen, denn betrachte z.B.

$$f(Z) := Z^p - Y \in K(Y)[Z].$$

Eisenstein mit $p = Y$ (Primelement, da irreduzibel!) liefert

$$f(Z) \in K[Y][Z]$$

irreduzibel.

$\xRightarrow[(f \text{ primitiv})]{\text{Gauß}}$ $f(Z) \in K(Y)[Z]$ irreduzibel.

Da $f(Z) = g(Z^p)$ gilt, mit $g(Z) = Z - Y$ besitzt f nach Vorlesung die mehrfache Nullstelle Y.

$\Rightarrow K(Y)$ ist nicht vollkommen.

- Sei nun $E := \overline{K(Y)}$ ein algebraischer Abschluss von $K(Y)$.

Ist F/E algebraische Erweiterung, dann folgt, da E algebraisch abgeschlossen ist: $F = E$

$\xRightarrow{\text{trivial}}$ F/E ist separabel.

$\Rightarrow E$ ist vollkommen.

- $E/K(Y)$ ist nach Konstruktion algebraisch, kann jedoch nicht separabel sein, da sonst nach (ii) $K(Y)$ vollkommen wäre.

Also: Haben algebraische Erweiterung $E/K(Y)$, welche nicht separabel ist mit: E ist vollkommen und $K(Y)$ ist nicht vollkommen.

$\Rightarrow$ In (ii) kann auf „E/K separabel" nicht verzichtet werden ▽

∎

3.4. Notation: Für einen Körper k und ein über k algebraisches Element α bezeichne stets $f_{\alpha,k}(X) \in k[X]$ das Minimalpolynom von α über k.

(i) Sei α separabel über K. Zu zeigen: $K[\alpha] = K[\alpha^p]$.

α separabel $\Rightarrow$ $f_{\alpha,K}(X)$ hat in einem algebraischen Abschluss $\overline{K}$ von K nur einfache Nullstellen.

In $K[\alpha^p][X]$ gilt, wenn wir $f_{\alpha,K}(X) \in K[\alpha^p][X]$ lesen wegen $f_{\alpha,K}(\alpha) = 0$:

$$f_{\alpha,K[\alpha^p]}(X) \mid f_{\alpha,K}(X)$$

$f_{\alpha,K}(X)$ besitzt nur einfache Nullstellen

$\Rightarrow$ $f_{\alpha,K[\alpha^p]}(X)$ besitzt nur einfache Nullstellen. (*)

Betrachte nun $g(X) := X^p - \alpha^p \in K[\alpha^p][X]$.

Wegen $g(\alpha) = 0$ folgt:

$$f_{\alpha,K[\alpha^p]}(X) \mid g(X)$$

Mit Frobenius folgt aber $g(X) = (X-\alpha)^p$, d.h. g besitzt nur α als Nullstelle. Wegen (*) muss daher gelten:

$$f_{\alpha,K[\alpha^p]}(X) = X - \alpha$$

(denn: $X-\alpha$ ist irreduzibel)

$\Rightarrow \alpha \in K[\alpha^p] \Rightarrow K[\alpha] = K[\alpha^p]$ (da offenbar $\alpha^p \in K[\alpha]$).

(ii) Gelte nun $K[\alpha] = K[\alpha^p]$. Wir zeigen, dass α separabel über K ist.

↗ α ist inseparabel über K.

$\Rightarrow$ $f_{\alpha,K}(X)$ hat in algebraischem Abschluss $\overline{K}$ von K mehrfache Nullstellen.

Sei $\deg f_{\alpha,K} =: n$.

$\overset{\text{vgl. 3.2.}}{\Rightarrow} \exists\, g \in K[X]$ mit $f_{\alpha,K}(X) = g(X^p)$ und $\deg g = \frac{n}{p}$

$\Rightarrow \alpha^p$ hat über K einen Grad $\leq \frac{n}{p}$.

Nun haben wir:

$$[K(\alpha) : K] = \deg f_{\alpha,K} = n$$
$$[K(\alpha^p) : K] \leq \deg g = \frac{n}{p}$$

$\overset{\text{insb.}}{\Rightarrow} K[\alpha] \neq K[\alpha^p]$ ↯ Voraussetzung $K[\alpha] = K[\alpha^p]$.

(beachte: α, α^p algebraisch über $K \Rightarrow K[\alpha] = K(\alpha)$, $K[\alpha^p] = K(\alpha^p)$)

Also muss α doch separabel über K sein.

▨