Aufgabe H10T1A5

Sei $L|K$ eine Körpererweiterung, $0 \neq \alpha \in L$ mit $L = K(\alpha)$ und $n \in \mathbb{N}$ die minimale natürliche Zahl mit $\alpha^n \in K$.

(a) Sei m eine natürliche Zahl mit $\alpha^m \in K$. Zeigen Sie, dass n ein Teiler von m ist.

(b) Sei $p = \mathrm{char}(K)$ eine Primzahl. Zeigen Sie: Ist $L|K$ separabel, dann gilt $p \nmid n$.

Lösung:

zu (a) Angenommen, n ist kein Teiler von m. Division mit Rest liefert $q, r \in \mathbb{Z}$ mit $m = qn + r$ und $0 \leq r \leq n$. Wegen $n \nmid m$ gilt sogar $0 < r < n$. Wir erhalten dann $\alpha^r = \alpha^{m-qn} = (\alpha^m)(\alpha^n)^{-q}$, und aus $\alpha^m, \alpha^n \in K$ folgt $\alpha^r \in K$. Aber dies widerspricht der Minimalität von n.

zu (b) Nehmen wir an, dass $L|K$ separabel, p aber ein Teiler von n ist. Sei $m \in \mathbb{N}$ mit $n = pm$, $\beta = \alpha^m$ und $f \in K[x]$ das Minimalpolynom von β über K. Weil β über K separabel ist, handelt es sich bei f um ein separables Polynom. Setzen wir $a = \alpha^n$, dann liegt a in K, und es gilt

$$\alpha^{pm} = a \quad \Leftrightarrow \quad (\alpha^m)^p = a \quad \Leftrightarrow \quad \beta^p - a = 0 \quad ,$$

also ist β eine Nullstelle von $g = x^p - a \in K[x]$ und f somit ein Teiler von g. Aus $\beta^p = a$ und $\mathrm{char}(K) = p$ folgt $g = x^p - \beta^p = (x - \beta)^p$. Ist f ein echter Teiler von g, dann muss f die Form $(x - \beta)^\ell$ für ein $\ell \in \mathbb{N}$ mit $1 \leq \ell < p$ haben. Bis auf Vorzeichen wäre der konstante Term von $f \in K[x]$ dann $(-\beta)^\ell$, also $\alpha^{\ell m} = \beta^\ell \in K$, was aber wegen $\ell m < n$ im Widerspruch zur Minimalität von n steht. Also ist $f = g$. Aber in diesem Fall ist die Ableitung von f gleich $f' = px^{p-1} = 0$. Dies widerspricht der Voraussetzung, dass f separabel ist, denn in diesem Fall ist $\mathrm{ggT}(f, f') = \mathrm{ggT}(f, 0) \neq 1$.