Aufgabe H19T2A5 (12 Punkte)

Sei K ein Körper der Charakteristik $p \neq 0$, seien $a \in K$ und $f = x^p - x - a \in K[x]$. Zeigen Sie:

(a) Sind L ein Erweiterungskörper von K und $b \in L$ eine Nullstelle von f, dann ist auch $b+1$ eine Nullstelle von f.

(b) Entweder hat f eine Nullstelle in K, oder f ist irreduzibel.

(c) Ist f irreduzibel, dann ist die Galoisgruppe von f eine zyklische Gruppe der Ordnung p.

Lösung:

zu (a) Wegen $\mathrm{char}(K) = p$ gilt $(c+d)^p = c^p + d^p$ für alle $c, d \in K$. Ist nun $b \in L$ ein Element mit $f(b) = 0$, dann folgt $f(b+1) = (b+1)^p - (b+1) - a = b^p + 1^p - b - 1 - a = b^p - b - a = f(b) = 0$.

zu (b) Nehmen wir an, dass f weder irreduzibel in K ist noch in K eine Nullstelle besitzt. Dann hat f einen über K irreduziblen Faktor $g \in K[x]$ mit $1 < \mathrm{grad}(g) < \mathrm{grad}(f)$. Sei K^{alg} ein algebraischer Abschluss von K und $\alpha \in K^{\mathrm{alg}}$ eine Nullstelle von g. Dann ist α auch eine Nullstelle von f. Nach Teil (a) ist mit α auch $\alpha + 1$ eine Nullstelle von f; durch wiederholte Anwendung von (a) kommen wir zu dem Ergebnis, dass die Menge $N = \{\alpha + \ell \mid 0 \leq \ell < p\}$ aus lauter Nullstellen von f besteht. Die Menge enthält p verschiedene Elementen, denn wegen $\mathrm{char}(K) = p$ gilt für alle $k, \ell \in \mathbb{Z}$ mit $0 \leq k < \ell < p$ jeweils $0 \leq \ell - k < p$ und damit $(\alpha + \ell) - (\alpha + k) = \ell - k \neq 0$ im Körper K. Da f als Polynom von Grad p über einem Körper nicht mehr als p Nullstellen haben kann, muss N die Nullstellenmenge von f in K^{alg} sein.

Wegen $\mathrm{grad}(g) > 1$ besitzt g neben α noch mindestens eine weitere Nullstelle $\beta \in K^{\mathrm{alg}}$ der Form $\beta = \alpha + \ell$ mit $1 \leq \ell < p$. Nach dem Fortsetzungssatz gibt es einen K-Homomorphismus $\sigma : K(\alpha) \to K^{\mathrm{alg}}$ mit $\sigma(\alpha) = \beta = \alpha + \ell$. Wir zeigen nun durch vollständige Induktion, dass $\alpha + m\ell$ für jedes $m \in \mathbb{N}$ eine Nullstelle von g ist. Für $m = 1$ ist dies bereits bekannt. Ist nun $m \in \mathbb{N}$ beliebig und setzen wir die Aussage für m voraus, dann ist mit $\alpha + m\ell$ auch $\sigma(\alpha + m\ell)$ eine Nullstelle von g, denn es gilt $g \in K[x]$, und g ist ein K-Homomorphismus. Darüber hinaus gilt $\sigma^{m+1}(\alpha) = \sigma(\sigma^m(\alpha)) = \sigma(\alpha + m\ell) = \sigma(\alpha) + m\ell = \alpha + \ell + m\ell = \alpha + (m+1)\ell$. (Dabei wurde verwendet, dass mit $1 = 1_K$ auch $m\ell$ in K liegt und somit $\sigma(m\ell) = m\ell$ gilt.)

Daraus folgt, dass insbesondere die Elemente $\alpha + m\ell$ mit $0 \leq m < p$ alles Nullstellen von g sind. Diese Nullstellen sind alle voneinander verschieden. Sind nämlich $0 \leq m_1, m_2 < p$ mit $\alpha + m_1\ell = \alpha + m_2\ell$, dann folgt $m_1\ell = m_2\ell$ in K und wegen $\mathrm{char}(K) = p$ somit die Kongruenz $m_1\ell \equiv m_2\ell \bmod p$. Dies wiederum bedeutet, dass $m_1\ell + p\mathbb{Z}$ und $m_2\ell + p\mathbb{Z}$ im Restklassenring $\mathbb{Z}/p\mathbb{Z}$ übereinstimmen, also $(m_1 + p\mathbb{Z})(\ell + p\mathbb{Z}) = (m_2 + p\mathbb{Z})(\ell + p\mathbb{Z})$ gilt. Wegen $1 \leq \ell < p$ ist das Element $\ell + p\mathbb{Z}$ in $\mathbb{Z}/p\mathbb{Z}$ ungleich Null und somit invertierbar, weil p eine Primzahl und $\mathbb{Z}/p\mathbb{Z}$ somit ein Körper ist. Wir dürfen deshalb die Gleichung $(m_1 + p\mathbb{Z})(\ell + p\mathbb{Z}) = (m_2 + p\mathbb{Z})(\ell + p\mathbb{Z})$ mit $(\ell + p\mathbb{Z})^{-1}$ multiplizieren und erhalten $m_1 + p\mathbb{Z} = m_2 + p\mathbb{Z}$. Weil aber die Elemente $\{0, 1, ..., p-1\}$ ein Repräsentantensystem von $\mathbb{Z}/p\mathbb{Z}$ bilden, folgt daraus $m_1 = m_2$. Also besitzt das Polynom g mindestens p verschiedene Nullstellen in K^{alg}. Dies bedeutet $\mathrm{grad}(g) \geq p = \mathrm{grad}(f)$, was aber der Voraussetzung $\mathrm{grad}(g) < \mathrm{grad}(f)$ widerspricht. Unsere Annahmen von oben hat also zu einem Widerspruch geführt. Folglich ist f entweder irreduzibel, oder es hat in K eine Nullstelle.

zu (c) Wieder sei K^{alg} ein algebraischer Abschluss von K, und es sei $\alpha \in K^{\mathrm{alg}}$ eine Nullstelle von f. Wir zeigen, dass $K(\alpha)$ ein Zerfällungskörper von f über K und $K(\alpha)|K$ eine Galois-Erweiterung ist. Wie wir bereits in Teil (b) festgestellt haben, ist $N = \{\alpha + \ell \mid 0 \leq \ell < p\}$ die Nullstellenmenge von f in K^{alg}. Wegen $|N| = p = \mathrm{grad}(f)$ zerfällt f über $K(N)$ in Linearfaktoren. Also ist $K(N)$ ein Zerfällungskörper von f über K. Darüber hinaus gilt $K(\alpha) = K(N)$; die Inklusion „$\subseteq$“ ist wegen $\alpha \in N$ offensichtlich, andererseits ist mit α auch $\alpha + \ell$ mit $0 \leq \ell < p$, also ganz N in $K(\alpha)$ enthalten. Die Tatsache, dass $K(\alpha)$ Zerfällungskörper eines Polynoms f über K ist, zeigt, dass $K(\alpha)|K$ eine normale Erweiterung ist.

Wegen $f' = px^{p-1} - 1 = -1$ und $\mathrm{ggT}(f, f') = \mathrm{ggT}(f, -1) = 1$ ist f ein separables irreduzibles Polynom. Weil es außerdem normiert ist und $f(\alpha) = 0$ erfüllt, handelt es sich um das *Minimalpolynom* von α über K. Somit ist α über K separabel, und $K(\alpha)|K$ ist eine separable Körpererweiterung. Insgesamt ist damit nachgewiesen, dass es sich bei $K(\alpha)|K$ um eine Galois-Erweiterung handelt. Weil $K(\alpha)$ Zerfällungskörper von f über K ist, ist die Galoisgruppe von f über K durch $\mathrm{Gal}(f|K) = \mathrm{Gal}(K(\alpha)|K)$ gegeben. Darüber hinaus gilt $|\mathrm{Gal}(f|K)| = |\mathrm{Gal}(K(\alpha)|K)| = [K(\alpha) : K] = \mathrm{grad}(f) = p$, und als Gruppe von Primzahlordnung ist $\mathrm{Gal}(f|K)$ eine zyklische Gruppe.