Aufgabe H18T1A5 (12 Punkte)

Sei $K = \{0, 1, a, b\}$ ein Körper mit vier Elementen (0 sei das Nullelement, 1 das Einselement).

(a) Stellen Sie die Additions- und die Multiplikationstabelle von K auf.

(b) Sei $f = x^4 + x + 1 \in K[x]$. Zeigen Sie, dass f reduzibel ist.

(c) Bestimmen Sie den Grad des Zerfällungskörpers von f über K.

Lösung:

zu (a) Aus der Vorlesung ist bekannt, dass allgemein ein Körper mit p^n Elementen, wobei p eine Primzahl und $n \in \mathbb{N}$ ist, die Charakteristik p hat. Für den angegebenen Körper K folgt daraus $\mathrm{char}(K) = 2$ und somit $0 + 0 = 1 + 1 = a + a = b + b = 0$. Weil 0 das Nullelement ist, gilt außerdem $0 + 1 = 1$, $0 + a = a$ und $0 + b = b$. Die Summe $1 + a$ bestimmen wir mit dem Ausschlussprinzip: Aus $a + 1 = 0$ würde sich wegen $\mathrm{char}(K) = 2$ die Gleichung $a = -1 = 1$ ergeben, aus $a + 1 = 1$ würde $a = 0$ und aus $a + 1 = a$ würde $1 = 0$ folgen. Also bleibt $a + 1 = b$ als einzige Möglichkeit. Damit erhalten wir auch $a + b = a + (a + 1) = (a + a) + 1 = 0 + 1 = 1$. Berücksichtigt man nun noch, dass die Addition auf einem Körper stets kommutativ ist, so ergibt sich die folgende Additionstabelle.

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

Weil 0 das Nullelement von K ist, gilt $0 \cdot 0 = 0 \cdot 1 = 0 \cdot a = 0 \cdot b = 0$. Weil 1 das Einselement ist, gilt $1 \cdot 1 = 1$, $1 \cdot a = a$ und $1 \cdot b = b$. Das Element $a \cdot b$ ermitteln wir wiederum durch Ausschließen. Die Gleichung $a \cdot b = 0$ kann nicht gelten, weil K als Körper keine Nullteiler ungleich 0 besitzt. Aus $a \cdot b = a$ würde durch Multiplikation der Gleichung mit a^{-1} die Gleichung $b = 1$ folgen, und aus $a \cdot b = b$ würde sich ebenso $a = 1$ ergeben. Also verbleibt $a \cdot b = 1$ als einzige Möglichkeit, und damit erhalten wir wegen $b + 1 = a$ weiter $a \cdot a = a \cdot (b + 1) = a \cdot b + a \cdot 1 = 1 + a = b$. Berücksichtigen wir noch die Kommutativität der Multiplikaton auf K, so erhalten wir die Multiplikationstabelle

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

zu (b) [*Vorüberlegung:* Es fällt auf, dass das Polynom f bereits über dem zweielementigen Körper $P = \{0, 1\}$ definiert ist. Eine Nullstelle von f erzeugt wegen $\mathrm{grad}(f) = 4$ über P einen Körper mit $2^4 = 16$ Elementen. Dieser enthält einen Körper mit vier Elementen, also den Körper K (wenn wir annehmen, dass sich alles in einem festgewählten algebraischen Abschluss abspielt). Es folgt $K(\alpha) = P(\alpha)$. Aber der Erweiterungsgrad von $K(\alpha)|K$ kann nicht ebenfalls gleich 4 sein (was der Fall wäre, wenn f auch über K irreduzibel ist), denn dann hätte $K(\alpha)$ nicht 16, sondern $4^4 = 64$ Elemente).]

Sei P der Primkörper von K, und sei $\tilde{K}$ ein algebraischer Abschluss von K. Weiter sei $\alpha \in \tilde{K}$ eine Nullstelle von f. Wegen $\mathrm{char}(K) = 2$ gilt für den Primkörper P laut Vorlesung $|P| = 2$. Daraus folgt, dass P aus dem Null- und dem Einselement von K besteht, also $P = \{0, 1\}$ gilt. Nehmen wir nun an, dass f über K irreduzibel ist. Dann ist $f \in P[x]$ erst recht über P irreduzibel. Es gilt also $f = \mu_{P,\alpha}$ und somit $[P(\alpha) : P] = \mathrm{grad}(\mu_{P,\alpha}) \leq \mathrm{grad}(f) = 4$. Als P-Vektorraum der Dimension 4 besteht $P(\alpha)$ aus genau $|P|^4 = 2^4 = 16$ Elementen.

Der Körper $\tilde{K}$ ist zugleich algebraischer Abschluss von P. Nun gibt es laut Vorlesung im algebraischen Abschluss eines p-elementigen Körpers P für jedes $m \in \mathbb{N}$ genau einen Teilkörper P_m mit p^m Elementen, wobei p eine beliebige Primzahl bezeichnet, und es gilt die Äquivalenz $m \mid n \Leftrightarrow P_m \subseteq P_n$ für alle $m, n \in \mathbb{N}$. In unserer Situation gilt also $P(\alpha) = P_4$, $K = P_2$ und somit $K \subseteq P(\alpha)$ wegen $2 \mid 4$, damit insbesondere $K(\alpha) = P(\alpha)$. Für den Erweiterungsgrad $m = [K(\alpha) : K] = [P(\alpha) : K]$ gilt $2^4 = |P(\alpha)| = |K|^m = 4^m = 2^{2m}$ und somit $m = 2$. Aber weil f über K irreduzibel ist, muss $f = \mu_{K,\alpha}$ und somit $m = [K(\alpha) : K] = \mathrm{grad}(f) = 4$ gelten. Der Widerspruch zeigt, dass die angenommene Irreduziblität von f falsch ist.

Variante:
Man kann auch eine explizite Zerlegung von f über dem Körper K suchen. Zunächst überprüft man durch Einsetzen, dass f in K keine Nullstellen besitzt. Also muss f das Produkt zweier irreduzibler Faktoren $g, h \in K[x]$ vom Grad 2 sein. Setzen wir diese in der Form $g = x^2 + rx + s$ und $h = x^2 + tx + u$ mit $r, s, t, u \in K$ an, so erhält man mit

$$x^4 + x + 1 \quad = \quad f \quad = \quad gh \quad = \quad (x^2 + rx + s)(x^2 + tx + u) \quad = \\ x^4 + (r + t)x^3 + (u + rt + s)x^2 + (ru + st)x + su$$

das Gleichungssystem $r + t = u + rt + s = 0$ und $ru + st = su = 1$. Durch Einsetzen von $t = -r = r$ vereinfacht es sich zu $u + r^2 + s = 0$, $r(u + s) = 1$ und $su = 1$. Auf Grund der letzten Gleichung gibt es für das Paar (s, u) nur die drei Möglichkeiten $(1, 1)$, (a, b) und (b, a). Die erste Möglichkeit ist ausgeschlossen, daraus würde $r(u+s) = r(1+1) = r \cdot 0 = 0$ folgen, im Widerspruch zu $r(u+s) = 1$. Die zweite Möglichkeit $(s, u) = (a, b)$ liefert $b + r^2 + a = 0 \Leftrightarrow r^2 + 1 = 0 \Leftrightarrow r^2 = 1 \Leftrightarrow r = 1$. Es wäre dann $g = x^2 + x + a$ und $h = x^2 + x + b$. Tatsächlich ist durch

$$(x^2 + x + a)(x^2 + x + b) \quad = \quad x^4 + (1 + 1)x^3 + (a + b + 1)x^2 + (a + b)x + ab \quad = \quad x^4 + x + 1$$

eine Zerlegung von f in zwei irreduzible Faktoren gegeben.

zu (c) Das Polynom f besitzt in K keine Nullstellen, denn es gilt $f(0) = 0^4 + 0 + 1 = 1 \neq 0$, $f(1) = 1^4 + 1 + 1 = 1 + 1 + 1 = 1 \neq 0$, $f(a) = a^4 + a + 1 = (a^2)^2 + a + 1 = b^2 + a + 1 = a + a + 1 = 1 \neq 0$ und $f(b) = b^4 + b + 1 = (b^2)^2 + b + 1 = a^2 + b + 1 = b + b + 1 = 1 \neq 0$. Da f andererseits nach Teil (b) über K reduzibel ist, besitzt f eine Darstellung als Produkt zweier normierter irreduzibler Faktoren $g, h \in K[x]$ mit $\mathrm{grad}(g) = \mathrm{grad}(h) = 2$. Sei nun wieder $\tilde{K}$ ein algebraischer Abschluss von K, und seien $\alpha, \beta \in \tilde{K}$ Nullstellen von g bzw. h. Wegen $\mathrm{grad}(g) = 2$ zerfällt g über $K(\alpha)$ in Linearfaktoren, aus demselben Grund das Polynom h über $K(\beta)$, und das Polynom $f = gh$ über $K(\alpha, \beta)$. Außerdem gilt $\mu_{K,\alpha} = g$, $\mu_{K,\beta} = h$, also $[K(\alpha) : K] = \mathrm{grad}(g) = 2$ und ebenso $[K(\beta) : K] = \mathrm{grad}(h) = 2$. Weil K ein endlicher Körper ist, existiert für jedes $d \in \mathbb{N}$ genau ein Zwischenkörper K_d von $\tilde{K}|K$ mit $[K_d : K] = d$. Somit gilt $K(\alpha) = K(\beta) = K(\alpha, \beta)$, also zerfällt f bereits über $K(\alpha)$ in Linearfaktoren. Außerdem wird $K(\alpha)$ über K von den Nullstellen des Polynoms f erzeugt, weil $K(\alpha)$ über K bereits allein von α erzeugt wird. Insgesamt ist also $K(\alpha)$ der Zerfällungskörper von f über K, und der gesuchte Erweiterungsgrad ist $[K(\alpha) : K] = 2$.