Algebra - Blatt 12 - Lösungsvorschlag

A1 (a) **wahr**. Setze $L = K(a^2)$ und $M = L(a) = K(a^2, a) = K(a)$.

Da a algebraisch über $L = K(a^2)$ ist (mit Minimalpoly $f(x) = x^2 - a^2$ falls $a \notin L$), ist $[M:L] < \infty$ (genauer: $[M:L] \leq 2$) nach Satz 3.2.5. ($M = L(a)$)

Nach Satz 3.1.6. ist damit $[M:K]$ endlich genau dann wenn $[L:K]$ endlich ist, ($M = K(a)$, $L = K(a^2)$)

d.h., nach Satz 3.2.5., dass a alg. über K ist gdw a^2 alg. über K ist.

Alternativ:

"$\Rightarrow$" Sei a alg. über K. Dann ist $K(a)/K$ algebraisch nach Satz 3.4.2, also ist $a^2 \in K(a)$ algebr. über K.

"$\Leftarrow$" Sei a^2 alg. über K, etwa $f \in K[X] \setminus \{0\}$, $f(a^2) = 0$. Setze $g(X) := f(X^2)$. Dann ist $g \in K[X] \setminus \{0\}$ mit $g(a) = f(a^2) = 0$, also ist a alg. über K.

(b) **falsch**. Ein Gegenbeispiel tauchte auf Blatt 11 auf:

$\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ hat Grad 4 über $\mathbb{Q}$ nach A4 (b) & (d), d.h. $\sqrt{2}+\sqrt{3}$ hat Grad 4 über $\mathbb{Q}$; aber $\sqrt{2}$ und $\sqrt{3}$ haben jeweils Grad 2 über $\mathbb{Q}$

(Beweis: Es gilt aber $[K(a+b):K] \leq [K(a):K] \cdot [K(b):K]$. (Bekannter Satz 3.2.9.)

(d) falsch. Wieder gibt es auf Blatt 11 ein Gegenbeispiel:
Für $K=\mathbb{Q}$ und $a=\sqrt[3]{2}$ ist $\mathrm{MiPo}_{a/K}(X)=X^3-2$
(Es ist irreduzibel nach Eisenstein mit $p=2$, normiert und hat $\sqrt[3]{2}$ als Nullstelle. Nach Satz 3.2.2. ist es damit schon das Minimalpolynom.), aber nach Blatt 11 A2 ist $\mathbb{Q}(\sqrt[3]{2}) \subsetneq \mathbb{R}$, kann also insbesondere nicht die Nullstellen $\zeta_3 \cdot \sqrt[3]{2}$ und $\zeta_3^2 \cdot \sqrt[3]{2}$ von $\mathrm{MiPo}_{a/K}$ enthalten, also auch nicht in Linearfaktoren zerfallen.

(c) falsch. Ist $a \in K$, so ist es algebraisch über K, aber $\mathrm{MiPo}_{a/K}(X) = X-a$ ist irreduzibel in $K[X]=K(a)[X]$
Konkretes Bsp: $a=0$: $\mathrm{MiPo}_{a/K}(X)=X$
oder $a=1$: $\mathrm{MiPo}_{a/K}(X)=X-1$.
(Bem: Ist $a \notin K$ alg. über K, so ist $\mathrm{MiPo}_{a/K}(X)$ nicht irred. in $K(a)[X]$, da a eine Nullst. ist.)

(c) wahr. Angenommen, a, $a+b$ sind algebraisch über K, b transzendent.
Variante 1: Dann ist $[K(a+b):K] < \infty$ und a ist auch alg. über $K(a+b)$ mit $[K(a+b)(a):K(a+b)] \leq [K(a):K] < \infty$.
Also ist $[\underbrace{K(a+b)(a)}_{=K(a,b)=K(b)(a)}:K] = [K(a+b)(a):K(a+b)] \cdot [K(a+b):K] < \infty$,
Da a auch alg. über $K(b)$ ist, ist $[K(b)(a):K(b)] < \infty$
und $\underbrace{[K(b)(a):K]}_{<\infty} = \underbrace{[K(b)(a):K(b)]}_{<\infty} \cdot \underbrace{[K(b):K]}_{=\infty} = \infty$ ↯

Variante 2: Nach Satz 3.4.2 ist $b \in K(a, a+b)$ algebraisch über K. ↯

A2) (a) Es ist $f(\bar{0}) = \bar{2}$, $f(\bar{1}) = \bar{1}^2 + \bar{2} = \bar{3} = (\overline{-1})^2 + \bar{2} = f(\overline{-1})$, $\overline{-1} = \overline{4}$

$f(\bar{2}) = \bar{2}^2 + \bar{2} = \bar{6} = \bar{1} = (\overline{-2})^2 + \bar{2} = f(\overline{-2}) = f(\bar{3})$,

also $f(a) \neq \bar{0}$ für alle $a \in \mathbb{F}_5$. Da $\deg(f) = 2$ ist f damit schon irreduzibel.

(b) Nach Satz 2.8.2 ist (f) ein maximales Ideal, da f irreduzibel ist (beachte, dass $\mathbb{F}_5[X]$ nach Bsp. 2.5.9 euklidisch und nach Satz 2.5.10 damit ein Hauptidealring ist, sodass wir 2.8.2 anwenden dürfen!). Nach Satz 2.8.3 ist $K := \mathbb{F}_5[X]/(f)$ damit ein Körper.

Nach Bsp. 2.2.8 lässt sich jedes Element von K eindeutig in der Form

$$a + bX + (f) \quad \text{schreiben, mit } a, b \in \mathbb{F}_5.$$

Dafür gibt es genau $\#\mathbb{F}_5^2 = 5^2 = 25$ Möglichkeiten, d.h. $\#K = 25$.

Wäre $\mathbb{Z}/n\mathbb{Z} \cong K$ für ein $n \in \mathbb{N}$, so müsste $n = 25$ sein (wegen $\#K = 25$ und $\#\mathbb{Z}/n\mathbb{Z} = n$). Aber K ist ein Körper (insbes.: nullteilerfrei), aber $\mathbb{Z}/25\mathbb{Z}$ hat Nullteiler ($\bar{5} \cdot \bar{5} = \overline{25} = \bar{0}$). Also ist $K \neq \mathbb{Z}/25\mathbb{Z}$, d.h. $K \not\cong \mathbb{Z}/n\mathbb{Z}$ für alle $n \in \mathbb{N}$.

(c) $f: \mathbb{F}_p \to \mathbb{F}_p$, $x \mapsto x^2$ erfüllt $f(\bar{1}) = \bar{1} = f(\overline{-1})$ mit $\bar{1} \neq \overline{-1}$, da $p \neq 2$. Nach dem Hinweis sind wir damit fertig.

(d) Sei $\bar{a}$ wie in (c). Wie in (b) ist $\mathbb{F}_p[X]/(X^2 - \bar{a})$ ein Körper mit p^2 Elementen

A3 (a) Es ist $(g_1+g_2)^p = \sum_{k=0}^{p} \binom{p}{k} g_1^k \cdot g_2^{p-k} =$

$= g_1^p + g_2^p + \sum_{k=1}^{p-1} \binom{p}{k} g_1^k g_2^{p-k} \equiv g_1^p + g_2^p \pmod p$

$\binom{p}{k}$ durch p teilbar, d.h. $\equiv 0 \bmod p$

(b) Es ist

$g(Y) = f(Y+1) = 1 + \underbrace{(Y+1)^p}_{= 1+Y\cdot g_1(Y)} + \underbrace{(Y+1)^{2p}}_{= 1+Y\cdot g_2(Y)} + \dots + \underbrace{(Y+1)^{(p-1)p}}_{= 1+Y\cdot g_{p-1}(Y)}$

für geeignete g_i, also

$a_0 = \underbrace{1+1+\dots+1}_{p \text{ mal}} = p$.

Da die g_i dabei jeweils $\deg(g_i) = i\cdot p - 1$ erfüllen, ist $g(Y) = p + \dots + Y^{(p-1)\cdot p}$, d.h.

$a_{p(p-1)} = 1$

(c) Nach (a) für $g_1(Y) = Y$ und $g_2(Y) = 1$ ist

$Y^p + 1 \equiv \underbrace{(Y+1)^p}_{= X^p} \bmod p$.

Nach (a) gilt außerdem

$(X-1)^{p^2} = \underbrace{((X-1)^p)^p}_{\equiv X^p - 1 \bmod p} \equiv (X^p-1)^p \bmod p \equiv (X^p)^p - 1 \bmod p$

$= X^{p^2} - 1$.

Weiter ist $f(X)\cdot(X^p-1) = f(X)\cdot X^p - f(X)$

$$= (X^p + X^{2p} + X^{3p} + \dots + X^{p\cdot p}) - 1 - (X^p - X^{2p} - \dots - X^{p(p-1)})$$

$$= X^{p^2} - 1.$$

Zusammen ergibt sich

$$g(Y)\cdot Y^p = f(Y+1)\cdot Y^p = f(X)\cdot Y^p \equiv f(X)\cdot(X^p-1) \bmod p$$

$$= X^{p^2}-1 \equiv (X-1)^{p^2} \bmod p = Y^{p^2}, \text{ d.h.}$$

$$g(Y)\cdot Y^p \equiv Y^{p^2} \bmod p.$$

$g(Y) \overset{da}{\equiv} Y^p \pmod p$

(d) Nach (b) & (c) ist $p \mid a_0$, $p^2 \nmid a_0$, $p \nmid a_{p(p-1)}$ und $a_i \equiv 0 \pmod p$ für $i = 1, \dots, p(p-1)-1$, sodass sich das Eisenstein-Kriterium (auf g) anwenden lässt (und zeigt, dass $g(Y)$ irreduzibel ist).

$f_i \notin K[X]^\times$ Wäre nun $f(X) = f(Y+1) = f_1(Y+1)\cdot f_2(Y+1)$ nicht irreduzibel, so wäre $g(Y) = f(X) = g_1(Y)\cdot g_2(Y)$, $g_1, g_2 \notin K[Y]^\times$, da $\deg(g_i) = \deg(f_i)$

(e) Für $h(X) = X^{p^2}-1$ ist $h(\zeta) = 0$, wegen $f(X)\cdot(X^p-1) = h(X)$ und $\zeta^p - 1 \neq 0$ muss daher $f(\zeta) = 0$ sein.

Außerdem ist f irreduzibel (nach (d)) und normiert, also nach Satz 3.2.2. bereits das Minimalpolynom von ζ.

(f) Falls doch wäre $\zeta \in L$ nach Satz 3.3.2. Insbesondere wäre dann nach Satz 3.2.10. der Grad $[\mathbb{Q}(\zeta):\mathbb{Q}]$ von ζ eine Zweierpotenz.

Aber $\deg(\zeta) = \deg(\mathrm{Min}_{\zeta,\mathbb{Q}}) = \deg(f) = p(p-1)$ ist für $p \neq 2$ keine Zweierpotenz.