M. Truong, M. Künzer

Algebra für Lehramt, SoSe 22

Lösung 12

Aufgabe 45 Sei $\mathbb{F}_8 := \mathbb{F}_2[X]/(X^3 + X + 1)$, sei $\beta := X + (X^3 + X + 1) \in \mathbb{F}_8$.

(1) Man bestimme das Minimalpolynom $\mu_{\beta^2+1,\mathbb{F}_2}(X) \in \mathbb{F}_2[X]$.

(2) Gibt es in $\mathbb{F}_8$ einen Teilkörper K mit $|K| = 4$?

(3) Gibt es in $\mathbb{F}_8$ ein Element u, dessen Minimalpolynom $\mu_{u,\mathbb{F}_2}(X)$ Grad 2 hat?

Lösung.
Zu (1). Wir schreiben $x := \beta^2 + 1$. Wir berechnen die ersten Potenzen von x.

$$\begin{array}{lcl} x^0 & = & 1 \\ x^1 & = & \beta^2 + 1 \\ x^2 & = & \beta^4 + 1 \;=\; \beta^2 + \beta + 1 \\ x^3 & = & \beta^4 + \beta^3 + \beta^2 + \beta^2 + \beta + 1 \;=\; \beta^2 + \beta \end{array}$$

Wir erkennen, daß (x^0, x^1, x^2) linear unabhängig ist über $\mathbb{F}_2$. Ferner erkennen wir, daß

$$x^3 + x^2 + 1 \;=\; 0$$

ist. Folglich ist

$$\mu_{\beta^2+1,\mathbb{F}_2}(X) \;=\; X^3 + X^2 + 1 \,.$$

Zu (2). *Annahme*, es gibt in $\mathbb{F}_8$ einen Teilkörper K mit $|K| = 4$.
Es ist $\mathbb{F}_2 = \{0, 1\} \subseteq K$. Also ist $\mathbb{F}_8 \,|\, K \,|\, \mathbb{F}_2$.
Wir schreiben $k := [K : \mathbb{F}_2]$. Da K ein k-dimensionaler Vektorraum über $\mathbb{F}_2$ ist, ist $4 = |K| = |\mathbb{F}_2^k| = 2^k$. Also ist

$$[K : \mathbb{F}_2] \;=\; k \;=\; 2 \,.$$

Es wird

$$3 \;=\; [\mathbb{F}_8 : \mathbb{F}_2] \;=\; [\mathbb{F}_8 : K] \cdot [K : \mathbb{F}_2] \;=\; [\mathbb{F}_8 : K] \cdot 2 \,.$$

Da $[\mathbb{F}_8 : K] \in \mathbb{Z}_{\geqslant 1}$, ist dies aber nicht möglich. Wir haben einen *Widerspruch.*
Also gibt es keinen solchen Teilkörper K.

Zu (3). *Annahme*, es gibt in $\mathbb{F}_8$ ein Element u, dessen Minimalpolynom $\mu_{u,\mathbb{F}_2}(X)$ Grad 2 hat. Wir betrachten den Teilkörper $K := \mathbb{F}_2(u) \subseteq \mathbb{F}_8$.
Es ist $[K : \mathbb{F}_2] = [\mathbb{F}_2(u) : \mathbb{F}_2] = \deg(\mu_{u,\mathbb{F}_2}(X)) = 2$. Das ist aber dank (2) nicht möglich. Wir haben einen *Widerspruch.*
Also gibt es kein solches Element u.

Aufgabe 46

(1) Man konstruiere einen Körper $\mathbb{F}_{25}$ mit $|\mathbb{F}_{25}| = 25$.

(2) Man bestimme in $\mathrm{U}(\mathbb{F}_{25})$ ein Element u, das nicht in $\mathbb{F}_5$ liegt, dessen Quadrat aber in $\mathbb{F}_5$ liegt. Ist $\mathrm{Syl}_2(\mathrm{U}(\mathbb{F}_{25})) = \{\langle u\rangle\}$?

(3) Man bestimme in $\mathrm{U}(\mathbb{F}_{25})$ ein Element der Ordnung 3.

(4) Sind die Ringe $\mathbb{F}_{25}$ und $\mathbb{Z}/(25)$ isomorph?

Lösung.
Zu (1). Es ist $X^2 - 2 \in \mathbb{F}_5[X]$ irreduzibel, da dieses Polynom Grad 2 hat und in $\mathbb{F}_5 = \{0, 1, 2, -2, -1\}$ keine Nullstelle hat.
Also ist
$$\mathbb{F}_{25} \;:=\; \mathbb{F}_5[X]/(X^2 - 2)$$
ein Körper mit $[\mathbb{F}_{25} : \mathbb{F}_5] = \deg(X^2 - 2) = 2$ und also $|\mathbb{F}_{25}| = |\mathbb{F}_5^2| = |\mathbb{F}_5|^2 = 25$.
Wir schreiben $\gamma := X + (X^2 - 5)$. Es ist $\mu_{\gamma,\mathbb{F}_5}(X) = X^2 - 5$. In
$$\mathbb{F}_{25} \;=\; \mathbb{F}_5(\gamma) \;=\; \{\, a + b\gamma \;:\; a,\, b \,\in\, \mathbb{F}_5 \,\}$$
ist also
$$5 \;=\; 0 \qquad \text{und} \qquad \gamma^2 \;=\; 2\;.$$

Zu (2). Sei $u := \gamma$. Dann ist $u \in \mathbb{F}_{25} \smallsetminus \mathbb{F}_5$. Es ist $u^2 = 2 \in \mathbb{F}_5$.
Es hat $u^2 = 2$ in $\mathrm{U}(\mathbb{F}_5) \leqslant \mathrm{U}(\mathbb{F}_{25})$ die Ordnung 4. Also hat u in $\mathrm{U}(\mathbb{F}_{25})$ die Ordnung 8.
Es ist $|\mathrm{U}(\mathbb{F}_{25})| = 25 - 1 = 24 = 2^3 \cdot 3$. Es ist $|\langle u\rangle| = 8$. Also ist $\langle u\rangle \in \mathrm{Syl}_2(\mathrm{U}(\mathbb{F}_{25}))$.
Es ist $\mathrm{U}(\mathbb{F}_{25})$ abelsch. Also ist $\langle u\rangle \trianglelefteq \mathrm{U}(\mathbb{F}_{25})$, da in $\mathrm{U}(\mathbb{F}_{25})$ jede Untergruppe ein Normalteiler ist. Folglich ist $\mathrm{Syl}_2(\mathrm{U}(\mathbb{F}_{25})) = \{\langle u\rangle\}$.

> Alternativ kann man auch anführen, daß in der zyklischen Gruppe $\mathrm{U}(\mathbb{F}_{25})$ von Ordnung 24 zu jedem Teiler d von 24 genau eine Untergruppe von Ordnung d existiert. Insbesondere gilt dies für $d = 8$. Also ist $\mathrm{Syl}_2(\mathrm{U}(\mathbb{F}_{25})) = \{\langle u\rangle\}$.

Zu (3). Sei versuchsweise $x := 1 + \gamma$. Wir berechnen Potenzen von x.
$$\begin{array}{rcl} x^0 & = & 1 \\ x^1 & = & 1 + \gamma \\ x^2 & = & 3 + 2\gamma \\ x^3 & = & 2 \\ x^4 & = & 2 + 2\gamma \end{array}$$
Da 2 die Ordnung 4 hat, ist $x^{12} = 1$. Es ist $x^4 \neq 1$, aber $(x^4)^3 = 1$. Also hat das Element
$$x^4 \;=\; 2 + 2\gamma$$
in $\mathrm{U}(\mathbb{F}_{25})$ die Ordnung 3.

> Was man auch durch eine direkte Rechnung bestätigen kann: $(2 + 2\gamma)^3 = 8(1 + \gamma)^3 = 3 \cdot 2 = 1$.

Zu (4). Es ist $\mathbb{F}_{25}$ ein Körper nach Konstruktion als Ring $\mathbb{F}_5[X]$ modulo dem maximalen Ideal $(X^2 - 5)$.
Es ist $\mathbb{Z}/(25)$ kein Körper, da in $\mathbb{Z}/(25)$ sich $5 \cdot 5 = 0$ ergibt, obwohl $5 \neq 0$ ist.
Also ist
$$\mathbb{F}_{25} \;\;\not\simeq\;\; \mathbb{Z}/(25)\;\;.$$

> Man kann auch $\mathrm{char}(\mathbb{F}_{25}) = 5$ und $\mathrm{char}(\mathbb{Z}/(25)) = 25$ als Grund dafür anführen, daß $\mathbb{F}_{25} \not\simeq \mathbb{Z}/(25)$.

Aufgabe 47

(1) Sei $L|K$ eine Körpererweiterung. Sei $\mathrm{Aut}(L|K)$ die Menge der Automorphismen von L über K. Man zeige: Es ist $\mathrm{Aut}(L|K)$ eine Untergruppe von S_L .

(2) Man bestimme $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})|\mathbb{Q})$.

(3) Man konstruiere einen Körper $\mathbb{F}_{27}$ mit $|\mathbb{F}_{27}| = 27$. Man bestimme $\mathrm{Aut}(\mathbb{F}_{27}|\mathbb{F}_3)$.

Lösung.
Zu (1). Seien $\varphi,\, \psi \,\in\, \mathrm{Aut}(L|K)$.
Wir zeigen $\varphi \circ \psi \overset{!}{\in} \mathrm{Aut}(L|K)$.
Es ist $(\varphi \circ \psi)(1) = \varphi(1) = 1$.

Es ist $(\varphi \circ \psi)(u+v) = \varphi(\psi(u)+\psi(v)) = \varphi(\psi(u)) + \varphi(\psi(v)) = (\varphi\circ\psi)(u) + (\varphi\circ\psi)(v)$ für $u,\, v \in L$.
Es ist $(\varphi \circ \psi)(u\cdot v) = \varphi(\psi(u)\cdot\psi(v)) = \varphi(\psi(u)) \cdot \varphi(\psi(v)) = (\varphi\circ\psi)(u) \cdot (\varphi\circ\psi)(v)$ für $u,\, v \in L$.
Es ist $(\varphi \circ \psi)(x) = \varphi(x) = x$ für $x \in K$.

Wir zeigen $\varphi^{-1} \overset{!}{\in} \mathrm{Aut}(L|K)$.
Es ist $\varphi^{-1}(1) = \varphi^{-1}(\varphi(1)) = 1$.
Es ist $\varphi^{-1}(u+v) = \varphi^{-1}(\varphi(\varphi^{-1}(u)) + \varphi(\varphi^{-1}(v))) = \varphi^{-1}(\varphi(\varphi^{-1}(u)+\varphi^{-1}(v))) = \varphi^{-1}(u)+\varphi^{-1}(v)$ für $u,\, v \in L$.
Es ist $\varphi^{-1}(u\cdot v) = \varphi^{-1}(\varphi(\varphi^{-1}(u)) \cdot \varphi(\varphi^{-1}(v))) = \varphi^{-1}(\varphi(\varphi^{-1}(u)\cdot\varphi^{-1}(v))) = \varphi^{-1}(u)\cdot\varphi^{-1}(v)$ für $u,\, v \in L$.
Es ist $\varphi^{-1}(x) = \varphi^{-1}(x)(\varphi(x)) = x$ für $x \in K$.
Also ist $\mathrm{Aut}(L|K) \leqslant \mathrm{S}_L$ gezeigt.
Insbesondere ist $\mathrm{Aut}(L|K)$, mit der Komposition $(\circ)$ als Multiplikation, eine Gruppe.

Zu (2). Es hat $\mu_{\sqrt{2},\mathbb{Q}}(X) = X^2 - 2$ in $\mathbb{Q}(\sqrt{2})$ die Nullstellen $\sqrt{2}$ und $-\sqrt{2}$.
Folglich haben wir beiden folgenden Elemente in $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})|\mathbb{Q})$.

$$\begin{array}{ccll} \mathbb{Q}(\sqrt{2}) & \overset{\mathrm{id}}{\underset{\sim}{\to}} & \mathbb{Q}(\sqrt{2}) & \\ f(\sqrt{2}) & \mapsto & f(\sqrt{2}) & \text{für } f(X) \in \mathbb{Q}[X] \end{array}$$

$$\begin{array}{ccll} \mathbb{Q}(\sqrt{2}) & \overset{\sigma}{\underset{\sim}{\to}} & \mathbb{Q}(\sqrt{2}) & \\ f(\sqrt{2}) & \mapsto & f(-\sqrt{2}) & \text{für } f(X) \in \mathbb{Q}[X] \end{array}$$

Wir behaupten, daß

$$\mathrm{Aut}(\mathbb{Q}(\sqrt{2})|\mathbb{Q}) \overset{!}{=} \{\mathrm{id}, \sigma\}$$

ist. Dazu genügt es zu zeigen, daß ein Automorphismus $\varphi \in \mathrm{Aut}(\mathbb{Q}(\sqrt{2})|\mathbb{Q})$ das Element $\sqrt{2}$ auf $\sqrt{2}$ oder auf $-\sqrt{2}$ schickt. Denn dann schickt er $f(\sqrt{2})$ auf $f(\sqrt{2})$ oder auf $f(-\sqrt{2})$ für $f(X) \in \mathbb{Q}[X]$, ist also gleich id oder gleich σ.
Es genügt also zu zeigen, daß $\varphi(\sqrt{2})$ eine Nullstelle von $\mu_{\sqrt{2},\mathbb{Q}}(X) = X^2 - 2$ ist.
Aber es ist

$$\mu_{\sqrt{2},\mathbb{Q}}(\varphi(\sqrt{2})) \;=\; \varphi(\sqrt{2})^2 - 2 \;=\; \varphi(\sqrt{2}-2) \;=\; \varphi(\mu_{\sqrt{2},\mathbb{Q}}(\sqrt{2})) \;=\; \varphi(0) \;=\; 0\,.$$

Zu (3). Es ist $X^3 - X + 1 \in \mathbb{F}_3[X]$ irreduzibel, da dieses Polynom von Grad 3 ist und keine Nullstellen in $\mathbb{F}_3 = \{0, 1, -1\}$ hat.
Also ist

$$\mathbb{F}_{27} \;:=\; \mathbb{F}_3[X]/(X^3 - X + 1)$$

ein Körper mit $[\mathbb{F}_{27} : \mathbb{F}_3] = \deg(X^3 - X + 1) = 3$ und also $|\mathbb{F}_{27}| = |\mathbb{F}_3^3| = |\mathbb{F}_3|^3 = 27$.
Wir schreiben $\varepsilon := X + (X^3 - X + 1)$. Es ist $\mu_{\varepsilon,\mathbb{F}_3}(X) = X^3 - X + 1$. In

$$\mathbb{F}_{27} \;=\; \mathbb{F}_3(\varepsilon) \;=\; \{\, a + b\varepsilon + c\varepsilon^2 \;:\; a,\, b,\, c \,\in\, \mathbb{F}_3 \,\}$$

ist also

$$3 \;=\; 0 \qquad \text{und} \qquad \varepsilon^3 \;=\; \varepsilon - 1\,.$$

Es ist der Frobeniusautomorphismus $\mathrm{Fr} = \mathrm{Fr}_{27} : \mathbb{F}_{27} \xrightarrow{\sim} \mathbb{F}_{27} : x \mapsto \mathrm{Fr}(x) = x^3$ ein Element von $\mathrm{Aut}(\mathbb{F}_{27}|\mathbb{F}_3)$.
Wir behaupten

$$\mathrm{Aut}(\mathbb{F}_{27}|\mathbb{F}_3) \;\overset{!}{=}\; \langle \mathrm{Fr} \rangle \;\overset{!}{=}\; \{\mathrm{Fr}^0, \mathrm{Fr}^1, \mathrm{Fr}^2\}\,.$$

Es ist $\mathrm{Fr}^0(\varepsilon) = \mathrm{id}(\varepsilon) = \varepsilon$.
Es ist $\mathrm{Fr}^1(\varepsilon) = \varepsilon^3 = -1 + \varepsilon$.
Es ist $\mathrm{Fr}^2(\varepsilon) = \varepsilon^9 = (-1+\varepsilon)^3 = (-1)^3 + \varepsilon^3 = -1 + (-1+\varepsilon) = 1 + \varepsilon$.
Es ist $\mathrm{Fr}^3(x) = x^{27} = x$ für $x \in \mathbb{F}_{27}$, da $\mathrm{U}(\mathbb{F}_{27}) = 27 - 1 = 26$ ist und daher $x^{26} = 1$ falls $x \neq 0$, mithin $x^{27} = x$ in jedem Fall.
Somit ist $\mathrm{Fr}^3 = \mathrm{id}$.

Alternativ kann man auch anführen, daß $\mathrm{Fr}^3(\varepsilon) = \varepsilon^{27} = (1+\varepsilon)^3 = 1^3 + \varepsilon^3 = \varepsilon$ ist, um $\mathrm{Fr}^3 = \mathrm{id}$ zu zeigen.

Es ist also tatsächlich Fr ein Element von Ordnung 3 in $\mathrm{Aut}(\mathbb{F}_{27}|\mathbb{F}_3)$ und somit $\langle \mathrm{Fr}\rangle \overset{!}{=} \{\mathrm{Fr}^0, \mathrm{Fr}^1, \mathrm{Fr}^2\}$.
Es bleibt zu zeigen, daß jedes Element $\varphi \in \mathrm{Aut}(\mathbb{F}_{27}|\mathbb{F}_3)$ in $\{\mathrm{Fr}^0, \mathrm{Fr}^1, \mathrm{Fr}^2\}$ liegt.
Es ist

$$\mu_{\varepsilon,\mathbb{F}_3}(\varphi(\varepsilon)) \;=\; \varphi(\varepsilon)^3 - \varphi(\varepsilon) + 1 \;=\; \varphi(\varepsilon^3 - \varepsilon + 1) \;=\; \varphi(0) \;=\; 0\,.$$

Also ist $\varphi(\varepsilon)$ eine Nullstelle von $X^3 - X + 1$.
Nun ist tatsächlich

$$\begin{array}{rcl} (X-\varepsilon)(X-(-1+\varepsilon))(X-(1+\varepsilon)) & = & (X-\varepsilon)((X-\varepsilon)+1)((X-\varepsilon)-1) \\ & = & (X-\varepsilon)((X-\varepsilon)^2-1) \\ & = & (X-\varepsilon)^3 - (X-\varepsilon) \\ & = & X^3 - \varepsilon^3 - X + \varepsilon \\ & = & X^3 - X + 1\,. \end{array}$$

Also hat $X^3 - X + 1$ nur die Nullstellen ε, $-1+\varepsilon$ und $1+\varepsilon$, also die Nullstellen $\mathrm{Fr}^0(\varepsilon)$, $\mathrm{Fr}^1(\varepsilon)$ und $\mathrm{Fr}^2(\varepsilon)$.
Somit ist $\varphi(\varepsilon) = \mathrm{Fr}^k(\varepsilon)$ für ein $k \in \{0,1,2\}$.
Also ist auch $\varphi(f(\varepsilon)) = f(\varphi(\varepsilon)) = f(\mathrm{Fr}^k(\varepsilon)) = \mathrm{Fr}^k(f(\varepsilon))$ für $f(X) \in \mathbb{F}_3[X]$.
Somit ist $\varphi = \mathrm{Fr}^k$.

Aufgabe 48 Wir schreiben $\zeta := \zeta_5 = \exp(\frac{2\pi i}{5})$. Wir betrachten die Körpererweiterung $\mathbb{Q}(\zeta)|\mathbb{Q}$.
Wir verwenden: $\mu_{\zeta,\mathbb{Q}}(X) = X^4 + X^3 + X^2 + X + 1 = \frac{X^5-1}{X-1}$.

(1) Man bestimme eine $\mathbb{Q}$-lineare Basis von $\mathbb{Q}(\zeta)$. Man bestimme $[\mathbb{Q}(\zeta):\mathbb{Q}]$.

(2) Man bestimme $\mu_{\zeta+\zeta^{-1},\mathbb{Q}}(X)$.

(3) Man zeige: $\mu_{\zeta-1,\mathbb{Q}}(X) = \mu_{\zeta,\mathbb{Q}}(X+1)$. Man bestimme $\mu_{\zeta-1,\mathbb{Q}}(X)$.

Lösung.
Zu (1). Es ist $(\zeta^0, \zeta^1, \zeta^2, \zeta^3)$ eine $\mathbb{Q}$-lineare Basis von $\mathbb{Q}(\zeta)$, da $3 = \deg(\mu_{\zeta,\mathbb{Q}}(X)) - 1$.
Es ist $[\mathbb{Q}(\zeta):\mathbb{Q}] = \deg(\mu_{\zeta,\mathbb{Q}}(X)) = 4$.

Zu (2). Sei $x := \zeta + \zeta^{-1}$.
Da $\zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 = 0$, ist $-\zeta^3 - \zeta^2 - \zeta - 1 = \zeta^{-1}$.
Wir berechnen Potenzen von x.

$$\begin{array}{rcl} x^0 & = & 1 \\ x^1 & = & \zeta + \zeta^-1 \;=\; -1 - \zeta^2 - \zeta^3 \\ x^2 & = & (-1-\zeta^2-\zeta^3)^2 \;=\; 1 + \zeta^4 + \zeta^6 + 2\zeta^2 + 2\zeta^3 + 2\zeta^5 \;=\; 3 + \zeta^4 + \zeta + 2\zeta^2 + 2\zeta^3 \;=\; 2 + \zeta^2 + \zeta^3\,. \end{array}$$

Es ist (x^0, x^1) linear unabhängig über $\mathbb{Q}$. Es ist $x^2 + x - 1 = 0$. Also ist

$$\mu_{\zeta+\zeta^{-1},\mathbb{Q}}(X) \;=\; X^2 + X - 1\,.$$

Zu (3). Es ist $\mu_{\zeta,\mathbb{Q}}(X) \in \mathbb{Q}[X]$ irreduzibel. Mit Translation ist also auch $\mu_{\zeta,\mathbb{Q}}(X+1) \in \mathbb{Q}[X]$ irreduzibel.
Es ist $\mu_{\zeta,\mathbb{Q}}(X+1)$ normiert.
Es ist $\mu_{\zeta,\mathbb{Q}}((\zeta-1)+1) = \mu_{\zeta,\mathbb{Q}}(\zeta) = 0$.
Also ist $\mu_{\zeta-1,\mathbb{Q}}(X) = \mu_{\zeta,\mathbb{Q}}(X+1)$.
Es ist $\mu_{\zeta,\mathbb{Q}}(X) \cdot (X-1) = X^5 - 1$.
Also ist $\mu_{\zeta,\mathbb{Q}}(X+1) \cdot ((X+1)-1) = (X+1)^5 - 1$.
Mit anderen Worten, es ist $\mu_{\zeta,\mathbb{Q}}(X+1) \cdot X = X^5 + 5X^4 + 10X^3 + 10X^2 + 5X + 1 - 1$.
Also ist

$$\mu_{\zeta-1,\mathbb{Q}}(X) \;=\; \mu_{\zeta,\mathbb{Q}}(X+1) \;=\; X^4 + 5X^3 + 10X^2 + 10X + 5\,.$$

Man kann auch das Eisenstein-Kriterium für die Irreduzibilität von $\mu_{\zeta,\mathbb{Q}}(X+1)$ heranziehen.