N. Krauß, M. Künzer

Algebra für Lehramt, SoSe 21

Lösung 10

Aufgabe 37

(1) Man konstruiere einen Körper $\mathbb{F}_8$ mit 8 Elementen.

(2) Man bestimme eine $\mathbb{F}_2$-lineare Basis von $\mathbb{F}_8$ und den Grad $[\mathbb{F}_8 : \mathbb{F}_2]$ der Körpererweiterung $\mathbb{F}_8|\mathbb{F}_2$.

(3) Man erstelle die Additionstafel von $\mathbb{F}_8$.

(4) Man erstelle die Multiplikationstafel von $\mathbb{F}_8$.
Man gebe zu jedem Element in $\mathbb{F}_8^\times$ das multiplikative Inverse an.

Lösung zu Aufgabe 37:

(1) Wir konstruieren uns einen Körper $\mathbb{F}_8$ als Körpererweiterung von $\mathbb{F}_2$.

Es ist z.B. $m(X) = X^3 + X + 1 \in \mathbb{F}_2[X]$ irreduzibel, denn eine Zerlegung in einen Faktor von Grad 1 und einen Faktor von Grad 2 hätte eine Nullstelle in $\mathbb{F}_2$ zur Folge, die dieses Polynom aber nicht hat.

Dank Lemma 196 gibt es den Körper $\mathbb{F}_8 := \mathbb{F}_2[X]/(X^3+X+1)$. Sei $\beta := X+(X^3+X+1)$. Dann ist $\mathbb{F}_8 = \mathbb{F}_2(\beta)$ und $\beta^3 = \beta + 1$.

Es liegen in der Tat 8 Elemente in $\mathbb{F}_2(\beta)$.

(2) Dank Lemma 195 hat $\mathbb{F}_2(\beta)$ die $\mathbb{F}_2$-lineare Basis $(\beta^0, \beta^1, \beta^2)$.

Insbesondere ist $[\mathbb{F}_2(\beta) : \mathbb{F}_2] = 3$.

Es ist also

$$\mathbb{F}_8 = \mathbb{F}_2(\beta) = \{a+b\beta+c\beta^2 : \ a,b,c \in \mathbb{F}_2\} = \{0, 1, \beta, 1+\beta, \beta^2, 1+\beta^2, \beta+\beta^2, 1+\beta+\beta^2\} \ .$$

(3) Wir erhalten folgende Additionstafel von $\mathbb{F}_8$.

$(+)$	0	1	β	$1+\beta$	β^2	$1+\beta^2$	$\beta+\beta^2$	$1+\beta+\beta^2$
0	0	1	β	$1+\beta$	β^2	$1+\beta^2$	$\beta+\beta^2$	$1+\beta+\beta^2$
1	1	0	$1+\beta$	β	$1+\beta^2$	β^2	$1+\beta+\beta^2$	$\beta+\beta^2$
β	β	$1+\beta$	0	1	$\beta+\beta^2$	$1+\beta+\beta^2$	β^2	$1+\beta^2$
$1+\beta$	$1+\beta$	β	1	0	$1+\beta+\beta^2$	$\beta+\beta^2$	$1+\beta^2$	β^2
β^2	β^2	$1+\beta^2$	$\beta+\beta^2$	$1+\beta+\beta^2$	0	1	β	$1+\beta$
$1+\beta^2$	$1+\beta^2$	β^2	$1+\beta+\beta^2$	$\beta+\beta^2$	1	0	$1+\beta$	β
$\beta+\beta^2$	$\beta+\beta^2$	$1+\beta+\beta^2$	β^2	$1+\beta^2$	β	$1+\beta$	0	1
$1+\beta+\beta^2$	$1+\beta+\beta^2$	$\beta+\beta^2$	$1+\beta^2$	β^2	$1+\beta$	β	1	0

(4) Wir erhalten folgende Multiplikationstafel von $\mathbb{F}_8$.

$(\cdot)$	0	1	β	$1+\beta$	β^2	$1+\beta^2$	$\beta+\beta^2$	$1+\beta+\beta^2$
0	0	0	0	0	0	0	0	0
1	0	1	β	$1+\beta$	β^2	$1+\beta^2$	$\beta+\beta^2$	$1+\beta+\beta^2$
β	0	β	β^2	$\beta+\beta^2$	$\beta+1$	1	$1+\beta+\beta^2$	$1+\beta^2$
$1+\beta$	0	$1+\beta$	$\beta+\beta^2$	$1+\beta^2$	$1+\beta+\beta^2$	β^2	1	β
β^2	0	β^2	$\beta+1$	$1+\beta+\beta^2$	$\beta+\beta^2$	β	$1+\beta^2$	1
$1+\beta^2$	0	$1+\beta^2$	1	β^2	β	$1+\beta+\beta^2$	$1+\beta$	$\beta+\beta^2$
$\beta+\beta^2$	0	$\beta+\beta^2$	$1+\beta+\beta^2$	1	$1+\beta^2$	$1+\beta$	β	β^2
$1+\beta+\beta^2$	0	$1+\beta+\beta^2$	$1+\beta^2$	β	1	$\beta+\beta^2$	β^2	$1+\beta$

Insbesondere haben wir folgende Inverse.

$x \in \mathbb{F}_8^\times$	1	β	$1+\beta$	β^2	$1+\beta^2$	$\beta+\beta^2$	$1+\beta+\beta^2$
$x^{-1} \in \mathbb{F}_8^\times$	1	$1+\beta^2$	$\beta+\beta^2$	$1+\beta+\beta^2$	β	$1+\beta$	β^2

Es gibt nur zwei irreduzible Polynome von Grad 3 in $\mathbb{F}_2[X]$. Nämlich X^3+X+1 und X^3+X^2+1. Wenn wir X^3+X^2+1 zur Konstruktion benutzt hätten, hätten wir einen Körper mit 8 Elementen $\mathbb{F}_2(\gamma)$ mit $\gamma^3 = \gamma^2+1$ erhalten, der isomorph zu $\mathbb{F}_2(\beta)$ ist. Es gibt den Körperisomorphismus $\mathbb{F}_2(\gamma) \to \mathbb{F}_2(\beta) : \beta \mapsto 1+\beta$. Es ist $1+\beta$ Nullstelle von X^3+X^2+1, da $(1+\beta)^3+(1+\beta)^2+1 = (1+\beta)^2(1+\beta+1)+1 = \beta + \underbrace{\beta^3}_{1+\beta} + 1 = 0$. Vgl. §3.9.

Aufgabe 38 Sei L ein Körper und $\alpha : L \to L$ ein Körpermorphismus.
Sei $\mathrm{Fix}_\alpha(L) := \{x \in L : \alpha(x) = x\}$ die Menge der Fixpunkte von L unter α.

(1) Man zeige: Es ist $\mathrm{Fix}_\alpha(L)$ ein Teilkörper von L.

(2) Man konstruiere einen Körper $\mathbb{F}_{25}$ mit 25 Elementen.

(3) Wir erinnern an den Frobenius-Endomorphismus $\mathrm{Fr} : \mathbb{F}_{25} \to \mathbb{F}_{25} : x \mapsto x^5$.
Man bestimme $\mathrm{Fix}_{\mathrm{Fr}}(\mathbb{F}_{25})$.

Lösung zu Aufgabe 38:

(1) Wir zeigen zunächst, dass $\mathrm{Fix}_\alpha(L)$ ein Teilring von L ist.

Es ist $1_L \in \mathrm{Fix}_\alpha(L)$, da α ein Körpermorphismus ist und daher $\alpha(1_L) = 1_L$ ist.

Seien $x, x' \in \mathrm{Fix}_\alpha(L)$.

Es ist $\alpha(x-x') = \alpha(x) - \alpha(x') = x - x'$ und daher auch $x - x' \in \mathrm{Fix}_\alpha(L)$.

Es ist $\alpha(x \cdot x') = \alpha(x) \cdot \alpha(x') = x \cdot x'$ und daher auch $x \cdot x' \in \mathrm{Fix}_\alpha(L)$.

Somit ist $\mathrm{Fix}_\alpha(L)$ ein Teilring von L.

Für $x \in \mathrm{Fix}_\alpha(L)^\times$ ist $1_L = \alpha(1_L) = \alpha(x \cdot x^{-1}) = \alpha(x) \cdot \alpha(x^{-1}) = x \cdot \alpha(x^{-1})$. Da das Inverse von x in L eindeutig festliegt, folgt $x^{-1} = \alpha(x^{-1})$ und daher $x^{-1} \in \mathrm{Fix}_\alpha(L)$.

Also ist $\mathrm{Fix}_\alpha(L)$ ein Teilkörper von L.

(2) Wir konstruieren uns einen Körper $\mathbb{F}_{25}$ als Körpererweiterung von $\mathbb{F}_5$.

Es ist z.B. $m(X) = X^2 - 2 \in \mathbb{F}_5[X]$ irreduzibel, denn eine Zerlegung in einen Faktoren von Grad 1 hätte eine Nullstelle in $\mathbb{F}_5$ zur Folge, die dieses Polynom aber nicht hat.

Dank Lemma 196 gibt es den Körper $\mathbb{F}_{25} := \mathbb{F}_5[X]/(X^2-2)$. Sei $\gamma := X + (X^2-2)$. Dann ist $\mathbb{F}_{25} = \mathbb{F}_5(\gamma)$ und $\gamma^2 = 2$.

Dank Lemma 195 hat $\mathbb{F}_5(\gamma)$ die $\mathbb{F}_5$-lineare Basis $(1, \gamma)$.

Insbesondere ist $[\mathbb{F}_5(\gamma) : \mathbb{F}_5] = 2$ und $|\mathbb{F}_5(\gamma)| = 5^2 = 25$. Daher nennen wir auch $\mathbb{F}_{25} := \mathbb{F}_5(\gamma)$.

Es ist also

$$\mathbb{F}_{25} = \{a + b\gamma : \ a, b \in \mathbb{F}_5\} \ .$$

(3) Sei $a + b\gamma \in \mathbb{F}_{25}$. Es ist $a + b\gamma \in \mathrm{Fix}_{\mathrm{Fr}}(\mathbb{F}_{25})$ genau dann, wenn $\mathrm{Fr}(a + b\gamma) \stackrel{!}{=} a + b\gamma$.

Es ist $\{x \in \mathbb{F}_5 : x^5 = x\} = \mathbb{F}_5$.

Zu erfüllen ist

$$\begin{aligned} \mathrm{Fr}(a + b\gamma) &= (a + b\gamma)^5 \\ &= a^5 + b^5\gamma^5 \\ &= a^5 - b^5\gamma \\ &= a - b\gamma \\ &\stackrel{!}{=} a + b\gamma \ . \end{aligned}$$

Koeffizientenvergleich liefert $b = 0$.

Daher folgt $\mathrm{Fix}_{\mathrm{Fr}}(\mathbb{F}_{25}) = \mathbb{F}_5 \subseteq \mathbb{F}_{25}$

Aufgabe 39 Sei $b := \sqrt[3]{5}$. Wir betrachten die Körpererweiterung $\mathbb{Q}(b)|\mathbb{Q}$.

(1) Man zeige mittels Descartes, dass $X^3 - 5 \in \mathbb{Q}[X]$ irreduzibel ist.
Man folgere, dass $\mu_{b,\mathbb{Q}}(X) = X^3 - 5$ ist.

(2) Man schreibe $(1+b)^{-1}$ als $\mathbb{Q}$-Linearkombination in der $\mathbb{Q}$-linearen Basis $(1, b, b^2)$ von $\mathbb{Q}(b)$.

(3) Man bestimme alle Körpermorphismen von $\mathbb{Q}(b)$ nach $\mathbb{C}$ über $\mathbb{Q}$.

(4) Man bestimme alle Körpermorphismen von $\mathbb{Q}(b)$ nach $\mathbb{Q}(b)$ über $\mathbb{Q}$.

Lösung zu Aufgabe 39:

(1) Wir zeigen mithilfe des Satzes von Descartes (Satz 10), dass $m(X) := X^3 - 5$ keine Nullstelle $a \in \mathbb{Q}$ besitzt.

Eine Nullstelle $a \in \mathbb{Q}$ muss von der Form $\frac{u}{v}$ sein, wobei $u, v \in \mathbb{Z}$ teilerfremd sind, u ein Teiler von 5 ist und v ein Teiler von 1 ist, d.h. es genügt $\frac{u}{v} \in \{-5, -1, 1, 5\}$ als mögliche Kandidaten zu betrachten.

Es ist $m(-5) = -130$, $m(-1) = -6$, $m(1) = -4$ und $m(5) = 120$. Somit hat $X^3 - 5$ keine Nullstelle $a \in \mathbb{Q}$, und kann folglich nicht in einen Faktor von Grad 1 und einen Faktor von Grad 2 zerfallen. Also ist $X^3 - 5$ irreduzibel in $\mathbb{Q}[X]$.

Es ist $b^3 - 5 = 5 - 5 = 0$, d.h. b ist Nullstelle von $m(X)$. Da $m(X)$ irreduzibel und normiert ist, folgt $\mu_{b,\mathbb{Q}}(X) = m(X) = X^3 - 5$.

(2) Wir suchen ein Element $a_0 + a_1 b + a_2 b^2 \in \mathbb{Q}(b)$ mit $a_0, a_1, a_2 \in \mathbb{Q}$ so, dass

$$(1+b) \cdot (a_0 + a_1 b + a_2 b^2) \stackrel{!}{=} 1$$

ist. Es ist

$$\begin{aligned} 1 \stackrel{!}{=} (1+b) \cdot (a_0 + a_1 b + a_2 b^2) &= a_0 + a_1 b + a_2 b^2 + a_0 b + a_1 b^2 + a_2 \underbrace{b^3}_{=5} \\ &= a_0 + 5a_2 + (a_0 + a_1) b + (a_1 + a_2) b^2 \ . \end{aligned}$$

Koeffizientenvergleich liefert das lineare Gleichungssystem

$$\begin{array}{lrcl} \text{(I)} & a_0 + 5a_2 &=& 1 \\ \text{(II)} & a_0 + a_1 &=& 0 \\ \text{(III)} & a_1 + a_2 &=& 0 \ . \end{array}$$

Aus (II) folgt $a_0 = -a_1$. Aus (III) folgt $a_2 = -a_1$. Damit folgt aus (I), dass $-6a_1 = 1$ ist, d.h. $a_1 = -\frac{1}{6}$, $a_0 = a_2 = \frac{1}{6}$.

Insgesamt ist

$$(1+b)^{-1} = \frac{1}{6}(1 - b + b^2) \ .$$

(3) Das Element $b \in \mathbb{Q}(b)$ erfüllt die Gleichung $b^3 - 5 = 0$. Für einen Körpermorphismus $\alpha : \mathbb{Q}(b) \to \mathbb{C}$ über $\mathbb{Q}$ muss daher

$$0 = \alpha(0) = \alpha(b^3 - 5) = \alpha(b)^3 - 5$$

gelten.

Da also $0 = \alpha(b)^3 - 5$ ist, folgt $\alpha(b) \in \{b,\, b \cdot \zeta_3,\, b \cdot \zeta_3^2\}$, wobei $\zeta_3 = \exp(\frac{2\pi \mathrm{i}}{3})$ ist.

Da $\mu_{b,\mathbb{Q}}(X) = X^3 - 5$ ist, gibt es nach Lemma 202 eindeutige Körpermorphismen $\alpha_1, \alpha_2, \alpha_3 : \mathbb{Q}(b) \to \mathbb{C}$ mit $\alpha_1(b) = b$, $\alpha_2(b) = b\zeta_3$ und $\alpha_3(b) = b\zeta_3^2$.

Es sind

$$\begin{array}{rcl} \alpha_1 : \mathbb{Q}(b) &\to& \mathbb{C} \\ a_0 + a_1 b + a_2 b^2 &\mapsto& a_0 + a_1 b + a_2 b^2 \ , \end{array}$$

$$\begin{array}{rcl} \alpha_2 : \mathbb{Q}(b) &\to& \mathbb{C} \\ a_0 + a_1 b + a_2 b^2 &\mapsto& a_0 + a_1 b\zeta_3 + a_2 b^2 \zeta_3^2 \ , \end{array}$$

und

$$\begin{array}{rcl} \alpha_3 : \mathbb{Q}(b) &\to& \mathbb{C} \\ a_0 + a_1 b + a_2 b^2 &\mapsto& a_0 + a_1 b\zeta_3^2 + a_2 b^2 \zeta_3 \ , \end{array}$$

wobei $a_0, a_1, a_2 \in \mathbb{Q}$.

(4) Jeder Körpermorphismus $\alpha : \mathbb{Q}(b) \to \mathbb{Q}(b)$ liefert durch Komponieren mit der Einbettung $\mathbb{Q}(b) \to \mathbb{C}$ auch ein Körpermorphismus von $\mathbb{Q}(b) \to \mathbb{C}$. Es genügt also, die in Teil (3) ermittelten zu betrachten.

Es ist $\mathbb{Q}(b) \subseteq \mathbb{R}$. Es ist $\alpha_2(\mathbb{Q}(b)) \not\subseteq \mathbb{R}$, da $\alpha_2(b) = b\zeta_3 \notin \mathbb{R}$. Es ist $\alpha_3(\mathbb{Q}(b)) \not\subseteq \mathbb{R}$, da $\alpha_3(b) = b\zeta_3^2 \notin \mathbb{R}$. Daher schränken α_2, α_3 nicht zu einem Automorphismus von $\mathbb{Q}(b)$ ein. Der Körpermorphismus α_1 hingegen schränkt zur Identität auf $\mathbb{Q}(b)$ ein, ist also der einzige Körpermorphismus von $\mathbb{Q}(b)$ nach $\mathbb{Q}(b)$ über $\mathbb{Q}$

Aufgabe 40 Wir betrachten die Körpererweiterung $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$.

(1) Man bestimme alle Körpermorphismen von $\mathbb{Q}(\sqrt{2})$ nach $\mathbb{Q}(\sqrt{2})$ über $\mathbb{Q}$.

(2) Man bestimme alle Körpermorphismen von $\mathbb{Q}(\sqrt{2})$ nach $\mathbb{Q}(\mathrm{i})$ über $\mathbb{Q}$.

(3) Man bestimme $\mu_{3+\sqrt{2},\mathbb{Q}}(X)$.

(4) Man bestimme $\{\deg(\mu_{y,\mathbb{Q}}(X)) : y \in \mathbb{Q}(\sqrt{2})\}$.

Lösung zu Aufgabe 40:

(1) Da $\sqrt{2} \notin \mathbb{Q}$ ist, ist X^2-2 irreduzibel in $\mathbb{Q}[X]$ und also $\mu_{\sqrt{2},\mathbb{Q}}(X) = X^2-2$. Es ist $(1, \sqrt{2})$ eine $\mathbb{Q}$-lineare Basis von $\mathbb{Q}(\sqrt{2})$, vgl. Aufgabe 7. Das Element $\sqrt{2}$ erfüllt die Gleichung $(\sqrt{2})^2 - 2 = 0$. Für einen Körpermorphismus $\alpha : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ muss daher

$$0 = \alpha(0) = \alpha((\sqrt{2})^2 - 2) = \alpha(\sqrt{2})^2 - 2$$

gelten.

Damit $0 = \alpha(\sqrt{2})^2 - 2$ ist, muss $\alpha(\sqrt{2}) \in \{-\sqrt{2}, \sqrt{2}\}$ sein.

Da $\mu_{\sqrt{2},\mathbb{Q}}(X) = X^2-2$ ist, gibt es nach Lemma 202 über $\mathbb{Q}$ eindeutige Körpermorphismen $\alpha_1, \alpha_2 : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ mit $\alpha_1(\sqrt{2}) = \sqrt{2}$ und $\alpha_2(\sqrt{2}) = -\sqrt{2}$.

Jedes Element $x \in \mathbb{Q}(\sqrt{2})$ lässt sich eindeutig schreiben als $x = a_0 + a_1\sqrt{2}$ mit $a_0, a_1 \in \mathbb{Q}$. Wir erhalten die folgenden Darstellungen für α_1, α_2.

$$\begin{array}{rcl} \alpha_1 : \mathbb{Q}(\sqrt{2}) & \to & \mathbb{Q}(\sqrt{2}) \\ a_0 + a_1\sqrt{2} & \mapsto & a_0 + a_1\sqrt{2} \end{array}$$

$$\begin{array}{rcl} \alpha_2 : \mathbb{Q}(\sqrt{2}) & \to & \mathbb{Q}(\sqrt{2}) \\ a_0 + a_1\sqrt{2} & \mapsto & a_0 - a_1\sqrt{2} \end{array}$$

(2) Das Element $\sqrt{2}$ erfüllt die Gleichung $(\sqrt{2})^2 - 2 = 0$. Für einen Körpermorphismus $\alpha : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\mathrm{i})$ muss daher

$$0 = \alpha(0) = \alpha((\sqrt{2})^2 - 2) = \alpha(\sqrt{2})^2 - 2$$

gelten.

Es ist $(1, \mathrm{i})$ eine $\mathbb{Q}$-lineare Basis von $\mathbb{Q}(\mathrm{i})$. Wir zeigen, es gibt kein Element $a_0 + a_1\mathrm{i} \in \mathbb{Q}(I)$ mit $(a_0 + a_1\mathrm{i})^2 = 2$.

Es ist $(a_0 + a_1\mathrm{i})^2 = a_0^2 + 2a_0a_1\mathrm{i} - a_1^2 = a_0^2 - a_1^2 + 2a_0a_1\mathrm{i} \stackrel{!}{=} 2 + 0 \cdot \mathrm{i}$. Koeffizientenvergleich liefert $2a_0a_1 = 0$, d.h. $a_0 = 0$ oder $a_1 = 0$. Dann folgt aber $a_0^2 = 2$ oder $-a_1^2 = 2$, aber beides ist unlösbar in $\mathbb{Q}$.

Somit kann es keinen Körpermorphismus $\mathbb{Q}(\sqrt{2})$ nach $\mathbb{Q}(\mathrm{i})$ über $\mathbb{Q}$ geben.

(3) Schreibe $x := 3 + \sqrt{2}$.

Es ist $x^2 = (3 + \sqrt{2})^2 = 9 + 6\sqrt{2} + 2 = 11 + 6\sqrt{2}$.

Es ist $x^2 - 6x = 11 + 6\sqrt{2} - 6(3 + \sqrt{2}) = -7$.

Somit ist $X^2 - 6X + 7$ ein Polynom, welches x als Nullstelle hat.

Es ist $X^2 - 6X + 7$ irreduzibel in $\mathbb{Q}[X]$, da $x \notin \mathbb{Q}$.

Also folgt $\mu_{3+\sqrt{2},\mathbb{Q}}(X) = X^2 - 6X + 7$.

(4) Es ist z.B. $\deg(\mu_{\sqrt{2},\mathbb{Q}}(X)) = 2$ und z.B. $\deg(\mu_{1,\mathbb{Q}}(X)) = \deg(X - 1) = 1$. Also ist

$$\{\deg(\mu_{y,\mathbb{Q}}(X)) : y \in \mathbb{Q}(\sqrt{2})\} \subseteq \{1, 2\}.$$

Angenommen, es gibt $y \in \mathbb{Q}(\sqrt{2})$ so, dass $\deg(\mu_{y,\mathbb{Q}}(X)) \geqslant 3$ ist. Dann gibt es einen Teilkörper $\mathbb{Q}(y) \subseteq \mathbb{Q}(\sqrt{2})$ mit $[\mathbb{Q}(y) : \mathbb{Q}] \geqslant 3$. Da $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ ist, ist das nicht möglich. *Widerspruch.*