Algebra Lösung Übungsblatt 10

Aufgabe 1 (3+3+3 Punkte).

Vor: Sei $K = \mathbb{Q}(\sqrt{2} - \sqrt{7})$.

a) **Beh:** $K = \mathbb{Q}(\sqrt{2}, \sqrt{7})$.

Bew: Es gilt $\sqrt{2} - \sqrt{7} \in \mathbb{Q}(\sqrt{2}, \sqrt{7})$, also ist $K \subset \mathbb{Q}(\sqrt{2}, \sqrt{7})$.

$$\begin{aligned}\sqrt{7} &= -\frac{1}{2}(-2\sqrt{7}) \\ &= -\frac{1}{2}(\sqrt{2} - \sqrt{7} - \sqrt{2} - \sqrt{7}) \\ &= -\frac{1}{2}(\sqrt{2} - \sqrt{7} + 5\frac{\sqrt{2} + \sqrt{7}}{-5}) \\ &= -\frac{1}{2}(\sqrt{2} - \sqrt{7} + 5\frac{\sqrt{2} + \sqrt{7}}{2-7}) \\ &= -\frac{1}{2}(\sqrt{2} - \sqrt{7} + 5\frac{1}{\sqrt{2} - \sqrt{7}}) \in K\end{aligned}$$

Damit folgt auch $\sqrt{2} = \sqrt{2} - \sqrt{7} + \sqrt{7} \in K$ und also $\mathbb{Q}(\sqrt{2}, \sqrt{7}) \subset K$. □

b) **Beh:** $\sqrt{7} \notin \mathbb{Q}(\sqrt{2})$ und $[K : \mathbb{Q}] = 4$.

Bew: Angenommen $\sqrt{7} \in \mathbb{Q}(\sqrt{2})$. Dann wäre $\sqrt{7} = a + b\sqrt{2}$ mit $a, b \in \mathbb{Q}$. Dann wäre $7 = a^2 + 2ab\sqrt{2} + 2b^2$. Wäre $a = 0$, so folgt $7 = 2b^2$. Widerspruch. Wäre $b = 0$ so wäre $7 = a^2$. Widerspruch. Dann muss also $a, b \neq 0$ und somit $\sqrt{2} = \frac{7-a^2-2b^2}{2ab}$. Widerspruch, da $a, b \in \mathbb{Q}$, $\sqrt{2} \notin \mathbb{Q}$.

Also $\sqrt{7} \notin \mathbb{Q}(\sqrt{2})$.

Um den Körpergrad von K über $\mathbb{Q}$ zu berechnen nutzen wir das Turmgesetz:

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$$

Es ist $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, und $[K : \mathbb{Q}(\sqrt{2})] \leq 2$, da $\sqrt{7}$ Nullstelle von $X^2 - 7 \in \mathbb{Q}(\sqrt{2})[X]$. Zudem gilt aber $[K : \mathbb{Q}(\sqrt{2})] \geq 2$, da $\sqrt{7} \notin \mathbb{Q}(\sqrt{2})$. Es folgt $[K : \mathbb{Q}] = 4$. □

c) **Gesucht:** Das Minimalpolynom von $\sqrt{2} - \sqrt{7}$ über $\mathbb{Q}$.

Lösung: Wir berechnen

$$\begin{aligned}(\sqrt{2} - \sqrt{7})^2 &= 9 - 2\sqrt{2}\sqrt{7} \\ (\sqrt{2} - \sqrt{7})^3 &= 23\sqrt{2} - 13\sqrt{7} \\ (\sqrt{2} - \sqrt{7})^4 &= 137 - 36\sqrt{2}\sqrt{7}\end{aligned}$$

Also ist $X^4 - 18X^2 + 25$ ein Polynom, das $\sqrt{2} - \sqrt{7}$ annulliert. Da es von Grad 4 ist, hat es den selben Grad wie das Minimalpolynom $\deg(m_{\sqrt{2}-\sqrt{7}}) = [K : \mathbb{Q}] = 4$. Außerdem ist es normiert, also $m_{\sqrt{2}-\sqrt{7}} = X^4 - 18X^2 + 25$.

Aufgabe 2 (3+3+3 Punkte + 2 Zusatzpunkte).

Konstruiere einen Körper mit 9 Elementen wie folgt:

Algebra Lösung Übungsblatt 10

1) **Beh:** $f := X^2 + 2X + 2 \in \mathbb{Z}_3[X]$ ist irreduzibel.

Bew: Da f vom Grad 2 ist, und $\mathbb{Z}_3$ ein Körper, können wir Aufgabe 4 von Blatt 9 verwenden. Also ist f irreduzibel über $\mathbb{Z}_3$, genau dann, wenn es über $\mathbb{Z}_3$ keine Nullstelle hat. Es gilt: $f(0) = 2, f(1) = 2, f(2) = 1$. Also hat f keine Nullstelle in $\mathbb{Z}_3$ und ist damit irreduzibel in $\mathbb{Z}_3[X]$. $\square$

2) **Gesucht:** Alle Elemente von $\mathbb{Z}_3[X]/\langle f \rangle$. Um wie viele Elemente handelt es sich?

Lösung: Da f Grad 2 hat, wissen wir, dass wir die Restklassen von Polynomen vom Grad größer gleich 2 durch Vertreter angeben können, die Polynome vom Grad maximal 1 sind. D.h. wir müssen die Restklassen aller Polynome vom Grad ≤ 1 durchgehen und auf Gleichheit überprüfen. Dann bekommen wir eine vollständige Liste der Elemente von $\mathbb{Z}_3[X]/\langle f \rangle$.

- $\bar{0} = \{a \cdot f | a \in \mathbb{Z}_3[X]\}$
- $\bar{1} = \{1 + a \cdot f | a \in \mathbb{Z}_3[X]\}$
- $\bar{2} = \{2 + a \cdot f | a \in \mathbb{Z}_3[X]\}$
- $\bar{X} = \{X + a \cdot f | a \in \mathbb{Z}_3[X]\}$
- $\overline{X+1} = \{X + 1 + a \cdot f | a \in \mathbb{Z}_3[X]\}$
- $\overline{X+2} = \{X + 2 + a \cdot f | a \in \mathbb{Z}_3[X]\}$
- $\overline{2X} = \{2X + a \cdot f | a \in \mathbb{Z}_3[X]\}$
- $\overline{2X+1} = \{2X + 1 + a \cdot f | a \in \mathbb{Z}_3[X]\}$
- $\overline{2X+2} = \{2X + 2 + a \cdot f | a \in \mathbb{Z}_3[X]\}$

Diese Restklassen sind alle paarweise verschieden, denn für zwei Vertreter $a_1X + a_0, b_1X + b_0$ folgt aus: $a_1X + a_0 = b_1X + b_0 + af$, dass $(a_1 - b_1)X + (a_0 - b_0) = af$. Dies ist eine Gleichheit in $\mathbb{Z}_3[X]$ und da $\deg(f) = 2$, muss $a = 0, a_1 = b_1, a_0 = b_0$.

Es ist also $|\mathbb{Z}_3[X]/\langle f \rangle| = 9$.

3) **Beh:** $(\mathbb{Z}_3[X]/\langle f \rangle, +, \cdot)$ ist ein Körper.

Bew: Wir schreiben die Verknüpfungstabellen auf. Für einfachere Notation schreiben wir definieren $\bar{w} = \overline{X}$ und zudem verzichten wir im folgenden auf die Restklassennotation.

+	0	1	2	w	w + 1	w + 2	2w	2w + 1	2w + 2
0	0	1	2	w	w + 1	w + 2	2w	2w + 1	2w + 2
1	1	2	0	w + 1	w + 2	w	2w + 1	2w + 2	2w
2	2	0	1	w + 2	w	w + 1	2w + 2	2w	2w + 1
w	w	w + 1	w + 2	2w	2w + 1	2w + 2	0	1	2
w + 1	w + 1	w + 2	w	2w + 1	2w + 2	2w	1	2	0
w + 2	w + 2	w	w + 1	2w + 2	2w	2w + 1	2	0	1
2w	2w	2w + 1	2w + 2	0	1	2	w	w + 1	w + 2
2w + 1	2w + 1	2w + 2	2w	1	2	0	w + 1	w + 2	w
2w + 2	2w + 2	2w	2w + 1	2	0	1	w + 2	w	w + 1

Wir sehen, dass $(\mathbb{Z}_3[X]/\langle f \rangle, +)$ eine abelsche Gruppe ist. Für die Multiplikative Tabelle überlegen wir uns zu erst folgendes:

$$X^2 = -(2X + 2) \pmod f = X + 1 \pmod f$$

$$X(X + 1) = X^2 + X = -(X + 2) \pmod f = 2X + 1 \pmod f$$

$$X(X + 2) = X^2 + 2X = -2 \pmod f = 1 \pmod f$$

Das heißt $w^2 = w + 1, w(w + 1) = 2w + 2, w(w + 2) = 1$. Daraus können wir alle weiteren Produkte folgern: $(w + 1)^2 = w^2 + 2w + 1 = (w + 1) + 2w + 1 = 2$ etc.

Algebra Lösung Übungsblatt 10

·	0	1	2	w	$w + 1$	$w + 2$	$2w$	$2w + 1$	$2w + 2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	w	$w + 1$	$w + 2$	$2w$	$2w + 1$	$2w + 2$
2	0	2	1	$2w$	$2w + 2$	$2w + 1$	w	$w + 2$	$w + 1$
w	0	w	$2w$	$w + 1$	$2w + 1$	1	$2w + 2$	2	$w + 2$
$w + 1$	0	$w + 1$	$2w + 2$	$2w + 1$	2	w	$w + 2$	$2w$	1
$w + 2$	0	$w + 2$	$2w + 1$	1	w	$2w + 2$	2	$w + 1$	$2w$
$2w$	0	$2w$	w	$2w + 2$	$w + 2$	2	$w + 1$	1	$2w + 1$
$2w + 1$	0	$2w + 1$	$w + 2$	2	$2w$	$w + 1$	1	$2w + 2$	w
$2w + 2$	0	$2w + 2$	$w + 1$	$w + 2$	1	$2w$	$2w + 1$	w	2

Es handelt sich also bei $(\mathbb{Z}_3[X]/\langle f \rangle, +, \cdot)$ um einen Körper mit 9 Elementen. □

4) **Zusatz**

Gegeben: Sei $\mathbb{F}_9 := \mathbb{Z}_3[X]/\langle f \rangle$ der in 1)-3) konstruierte Körper.

Gesucht: Die Nullstellen von $X^3 + X^2 + X + 1 \in \mathbb{F}_9[X]$ in $\mathbb{F}_9$ und eine Zerlegung in irreduzible Polynome.

Lösung: Wir verwenden für die Elemente aus $\mathbb{F}_9$ die Notation aus Teil 3), d.h. $\mathbb{F}_9 = \{0, 1, 2, w, w + 1, w + 2, 2w, 2w + 1, 2w + 2\}$. Wir sehen, dass $-1 = 2$ eine Nullstelle von $X^3 + X^2 + X + 1$ ist. Polynomdivision liefert nun:

$$X^3 + X^2 + X + 1 = (X - 2)(X^2 + 1)$$

Wir suchen also die Nullstellen von $X^2 + 1$ in $\mathbb{F}_9$. Wir schauen in die Multiplikationstabelle und suchen Elemente für die gilt $X^2 = -1 = 2$. Dies erfüllen genau die Elemente $w + 1$ und $2w + 2$. Das heißt wir haben für die Gleichung $X^2 + 1$ in $\mathbb{F}_9$ zwei Lösungen gefunden. Es folgt, dass wir $X^3 + X^2 + X + 1$ als Produkt von Linearfaktoren schreiben können:

$$X^3 + X^2 + X + 1 = (X - 2)(X - (w + 1))(X - (2w + 2)).$$

Insbesondere sehen wir hier, dass die Körpererweiterung $\mathbb{F}_9 = \mathbb{Z}_3[X]/\langle f \rangle$ die Quadratwurzeln zu $-1 = 2 \in \mathbb{Z}_3$ enthält.

Aufgabe 3 (3+3+3 Punkte).

Vor: Es sei $\zeta = e^{\frac{2\pi i}{7}} \in \mathbb{C}$ und $f = X^3 + X^2 - 2X - 1 \in \mathbb{Q}[X]$.

a) **Beh:** ζ ist Nullstelle von $\sum_{i=0}^6 X^i$.

Bew: Wir zeigen zunächst wie im Hinweis, dass ζ Nullstelle von $X^7 - 1$ ist:

$$\zeta^7 = e^{\frac{2\pi i}{7} \cdot 7} = e^{2\pi i} = 1$$

$\Rightarrow \zeta^7 - 1 = 0$ Nun ist aber auch 1 Nullstelle von $X^7 - 1$, sodass wir den Linearfaktor $X - 1$ abspalten können. Mit Polynomdivision erhalten wir:

$$X^7 - 1 = (X - 1) \left(\sum_{i=0}^6 X^i \right).$$

Da ζ keine Nullstelle von $X - 1$ folgt die Behauptung. □

b) **Beh:** $\alpha_1 := \zeta + \zeta^6$, $\alpha_2 := \zeta^2 + \zeta^5$ und $\alpha_3 := \zeta^3 + \zeta^4 \in \mathbb{R} \setminus \mathbb{Q}$ sind Nullstellen von f und f ist irreduzibel in $\mathbb{Q}[X]$.

Algebra Lösung Übungsblatt 10

Bew: Wir rechnen $f(\alpha_i)$ aus für $i = 1, 2, 3$.

$$\begin{aligned} f(\alpha_1) &= (\zeta + \zeta^6)^3 + (\zeta + \zeta^6)^2 - 2(\zeta + \zeta^6) - 1 \\ &= \zeta^3 + 3\zeta^2\zeta^6 + 3\zeta\zeta^{12} + \zeta^{18} + \zeta^2 + 2\zeta\zeta^6 + \zeta^{12} - 2\zeta - 2\zeta^6 - 1 \\ &= \zeta^3 + 3\zeta^8 + 3\zeta^{13} + \zeta^{18} + \zeta^2 + 2\zeta^7 + \zeta^{12} - 2\zeta - 2\zeta^6 - 1 \\ \text{da } \zeta^7 = 1 &= \zeta^3 + 3\zeta + 3\zeta^6 + \zeta^4 + \zeta^2 + 2 + \zeta^5 - 2\zeta - 2\zeta^6 - 1 \\ &= \zeta^6 + \zeta^5 + \zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 \\ \text{nach a)} &= 0. \end{aligned}$$

$$\begin{aligned} f(\alpha_2) &= (\zeta^2 + \zeta^5)^3 + (\zeta^2 + \zeta^5)^2 - 2(\zeta^2 + \zeta^5) - 1 \\ \text{da } \zeta^7 = 1 &= \zeta^6 + 3\zeta^2 + 3\zeta^5 + \zeta + \zeta^4 + 2 + \zeta^3 - 2\zeta^2 - 2\zeta^5 - 1 \\ &= \zeta^6 + \zeta^5 + \zeta^4 + \zeta^3 + \zeta^2 + 1 \\ \text{nach a)} &= 0. \end{aligned}$$

$$\begin{aligned} f(\alpha_3) &= (\zeta^3 + \zeta^4)^3 + (\zeta^3 + \zeta^4)^2 - 2(\zeta^3 + \zeta^4) - 1 \\ \text{da } \zeta^7 = 1 &= \zeta^2 + 3\zeta^3 + 3\zeta^4 + \zeta^5 + \zeta^6 + 2 + \zeta - 2\zeta^3 - 2\zeta^4 - 1 \\ &= \zeta^6 + \zeta^5 + \zeta^4 + \zeta^3 + \zeta^2 + \zeta + 1 \\ \text{nach a)} &= 0. \end{aligned}$$

Es bleibt noch zu zeigen, dass f irreduzibel ist über $\mathbb{Q}$. Da f Grad 3 hat, ist nach Blatt 9 Aufgabe 4 mit $K = \mathbb{Q}$ das Polynom $f \in \mathbb{Q}[X]$ irreduzibel über $\mathbb{Q}$, genau dann wenn f eine Nullstelle über $\mathbb{Q}$ hat. Aber die drei Nullstellen $\alpha_1, \alpha_2, \alpha_3$ sind nach Voraussetzung nicht in $\mathbb{Q}$. Daher ist f irreduzibel. $\square$

c) **Beh:** Das reguläre 7-Eck lässt sich nicht mit Zirkel und Lineal aus der Menge $\{0, 1\}$ konstruieren.

Bew: Um das regelmäßige 7-Eck zu konstruieren, muss man den Winkel $\frac{2\pi}{7} =: \theta$ konstruieren. Es ist $\zeta = \cos(\theta) + i\sin(\theta)$. Wäre das 7-Eck konstruierbar, so wären $\cos(\theta)$ und $\sin(\theta)$ konstruierbar, d.h. sie müssen in einer reellen Körpererweiterung vom Grad 2^n über $\mathbb{Q}$ liegen. (Satz 4.3.6).

Nach b) ist f das Minimalpolynom von $\alpha_1 = \zeta + \zeta^6 = \cos(\theta) + i\sin(\theta) + \cos(\theta) - i\sin(\theta) = 2\cos(\theta)$.

$\Rightarrow$ Da $\mathbb{Q}(\cos(\theta)) = \mathbb{Q}(2\cos(\theta))$, f das Minimalpolynom von $2\cos(\theta)$ und $\deg(f) = 3$ ist $[\mathbb{Q}(\cos(\theta)) : \mathbb{Q}] = 3 \neq 2^n$ für $n \in \mathbb{N}$.

$\Rightarrow \cos(\theta)$ ist nicht konstruierbar.

$\Rightarrow$ das regelmäßige 7-Eck ist nicht konstruierbar. $\square$