Anmerkungen und Lösungen zu

Einführung in die Algebra

Blatt 11

Jendrik Stelzner

Letzte Änderung: 20. Januar 2018

Aufgabe 1

(a)

Die Aussage ist *falsch*: Nach Aufgabe 2 von Zettel 10 gibt es einen Automorphismus $f\colon \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ mit $f(\sqrt{2}) = -\sqrt{2}$. Das Element $\sqrt{2} \in \mathbb{Q}(\sqrt[4]{2})$ hat eine Quadratwurzel, das Element $-\sqrt{2} \in \mathbb{Q}(\sqrt[4]{2})$ allerdings nicht. Es gibt deshalb keinen Körperhomomorphismus $\hat{f}\colon \mathbb{Q}(\sqrt[4]{2}) \to \mathbb{Q}(\sqrt[4]{2})$ mit $\hat{f}(\sqrt{2}) = -\sqrt{2}$. Daher lässt sich f nicht zu einem Körperhomomorphismus $\mathbb{Q}(\sqrt[4]{2}) \to \mathbb{Q}(\sqrt[4]{2})$ fortsetzen.

(b)

Die Aussage ist *falsch*: Nach dem Fundamentalsatz der Algebra zerfällt jedes normierte Polynom $f(t) \in \mathbb{R}[t]$ in quadratische und lineare Faktoren. Inbesondere ist $f(t)$ reduzibel, falls $\deg f(t) \geq 3$ gilt. Somit ist das gegebene Polynom reduzibel.

(c)

Die Aussage ist *wahr*: Eine einfache Lösung besteht darin, für $f(t)$ das konstante 1-Polynom zu wählen. Das Polynom $f(t)$ lässt sich aber auch nicht-konstant wählen: Gilt $S = \emptyset$, so lasst sich $f(t) = t$ wählen, und gilt $S \neq \emptyset$, so lässt sich $f(t) = 1 + \prod_{s \in S}(t - s)$ wählen.

(d)

Die Aussage ist *falsch*, da es keine endlichen algebraisch abgeschlossenen Körper gibt: Ist K ein endlicher Körper, so gibt es nach dem vorherigen Aufgabenteil ein nicht-konstantes Polynom $f(t) \in K[t]$ gibt, das in K keine Nullstelle hat.

(e)

Die Aussage ist *wahr*: Ist K ein endlicher Integritätsbereich, so ist K per Definition kommutative und es gilt $K \neq 0$. Es bleibt daher zu zeigen, dass jedes Element $x \in K$, $x \neq 0$ ein Inverses besitzt.

Die Abbildung $\lambda_x \colon K \to K$, $y \mapsto xy$ ist injektiv, da K ein Integritätsbereich ist, denn für alle $y_1, y_2 \in K$ gilt

$$\begin{aligned}\lambda_x(y_1) = \lambda_x(y_2) \implies xy_1 = xy_2 &\implies x(y_1 - y_2) = 0 \\ &\implies y_1 - y_2 = 0 \implies y_1 = y_2 \,.\end{aligned}$$

Wegen der Endlichkeit von K ist λ_x somit auch surjektiv. Inbesondere gibt es ein Element $y \in K$ mit $1 = \lambda_x(y) = xy$, so dass x eine Einheit in K ist.

Bemerkung 1. Ist $D \neq 0$ ein (nicht notwendigerweise kommutativer) links- und rechtsnullteilerfreier Ring, so ergibt sich nach der obigen Argumentation, dass jedes Element $x \in D$, $x \neq 0$ ein Links- und Rechtsinverses besitzt, und somit bereits ein beidseitig Inverses (der Leser sollte sich bewusst machen, dass diese Folgerung nicht trivial ist). Also ist D ein Schiefkörper.

Nach dem Satz von Wedderburn, ist jeder endliche Schiefkörper bereits kommutativ, und somit ein Körper. Dies gilt insbesondere für D.

Aufgabe 2

(a)

Da $\mathbb{Q} \subseteq K$ der Primkörper von K ist, gilt für den Körperhomomorphismus f, dass $f|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$. Für das Minimalpolynom $m_a(t) = \sum_i p_i t^i \in \mathbb{Q}[t]$ gilt $p_i \in \mathbb{Q}$ für alle i; für jede Nullstelle $b \in S_a$ von $m_a(t)$ gilt somit

$$m_a(f(b)) = \sum_i p_i f(b)^i = \sum_i f(p_i) f(b)^i = f\left(\sum_i p_i b^i\right) = f(m_a(b)) = f(0) = 0\,,$$

und somit auch $f(b) \in S_a$.

(b)

Für jedes $a \in K$ ist die Menge S_a endlich, da das Polynom $m_a(t) \in \mathbb{Q}[t] \subseteq K[t]$ nur endlich viele Nullstellen hat. Die Einschränkung $f|_{S_a}^{S_a} \colon S_a \to S_a$ ist injektiv, da f als Körperhomomorphismus injektiv ist, und wegen der Endlichkeit von S_a somit auch surjektiv. Also gilt $f(S_a) = S_a$.

(c)

Für jedes $a \in K$ gilt $a \in S_a$, weshalb $K = \bigcup_{a \in K} S_a$ gilt. Damit folgt, dass

$$f(K) = f\left(\bigcup_{a \in K} S_a\right) = \bigcup_{a \in K} f(S_a) = \bigcup_{a \in K} S_a = K$$

gilt. Somit ist der Körperhomomorphismus f surjektiv, und somit bereits ein Körperisomorphismus (als Körperhomomorphismus ist f insbesondere injektiv).

Aufgabe 3

(a)

Mit $f(t) = \sum_i a_i t^i$ und $g(t) = \sum_i b_i t^i$ gilt $(r \cdot f + s \cdot g)(t) = \sum_i (r \cdot a_i + s \cdot b_i) t^i$, und somit

$$\begin{aligned}(r \cdot f + s \cdot g)'(t) = \sum_i i(r \cdot a_i + s \cdot b_i) t^{i-1} &= r \cdot \sum_i i a_i t^{i-1} + r \cdot \sum_i i b_i t^{i-1} \\ &= r \cdot f'(t) + s \cdot g'(t)\,.\end{aligned}$$

(b)

Mit $f(t) = \sum_i a_i t^i$ und $g(t) = \sum_j b_j t^j$ gilt $(f \cdot g)(t) = \sum_{i,j} a_i b_j t^{i+j}$ und somit

$$\begin{aligned}(f \cdot g)'(t) &= \sum_{i,j} a_i b_j (i+j) t^{i+j-1} = \sum_{i,j} a_i b_j i t^{i+j-1} + \sum_{i,j} a_i b_j j t^{i+j-1} \\ &= \left(\sum_i a_i i t^{i-1}\right)\left(\sum_j b_j t^j\right) + \left(\sum_i a_i t^i\right)\left(\sum_j b_j j t^{j-1}\right) \\ &= f'(t) \cdot g(t) + f(t) \cdot g'(t)\,.\end{aligned}$$

(c)

Hat $f(t)$ keine 9 verschiedenen Nullstellen, so hat $f(t)$ in $\mathbb{F}_9$, und somit auch in $\overline{\mathbb{F}_3}$ eine mehrfache Nullstelle. Da $f(t)$ irreduzibel ist, gilt somit (wie in der Vorlesung gezeigt), dass $f'(t) = 0$. Insbesondere ist dann jedes $x \in \mathbb{F}_9$ eine Nullstelle von $f'(t)$.

(d)

Mit „doppelten“ Nullstellen sind in dieser Aufgaben die mehrfachen Nullstellen gemeint.

(i)

Für das gegebene Polynom $f(t) \coloneqq t^6 + t^5 - t^4 - t^3 - t^2 + t$ gilt

$$f'(t) = 5t^4 - 4t^3 - 2t + 1 = 2t^4 + 2t^3 + t + 1 = t^4 + t^3 + 2t + 2\,.$$

Es gibt nun (mindestens) zwei Vorgehensweisen: Wir bestimmen jeweils die gemeinsamen Nullstellen von $f(t)$ und $f'(t)$; dies sind dann genau die mehrfachen Nullstellen von $f(t)$ und $f'(t)$.

- Es gilt

  $$\begin{aligned} f'(t) &= t^4 + t^3 + 2t + 2 = t^3(t+1) + 2(t+1) \\ &= (t^3+2)(t+1) = (t+2)^3(t+1) = (t-1)^3(t-1)\,. \end{aligned}$$

  (Dabei nutzen wir für die Umfomung $(t^3+2) = (t+2)^3$, dass $\operatorname{char}(\mathbb{F}_9) = 3$ gilt.) Also zerfällt $f'(t)$ bereits über $\mathbb{F}_3$ in Linearfaktoren, und die auftretenden Nullstellen sind 1 und -1. Dabei ist 1 auch eine Nullstelle von $f(t)$, -1 hingegen nicht.

  Somit ist 1 die einzige gemeinsame Nullstelle von $f(t)$ und $f'(t)$, und somit auch die einzige mehrfache Nullstelle von $f(t)$.

- Mithife des euklidischen Algorithmus ergibt sich, dass $(t-1)^3$ der größte gemeinsame Teiler von $f(t)$ und $f'(t)$ ist. Da die gemeinsamen Nullstellen von $f(t)$ und $f'(t)$ genau die Nullstellen dieses größten gemeinsamen Teilers sind, ist 1 die einzige mehrfache Nullstelle des Polynoms $f(t)$.

(e)

Für das gegebene Polynom $g(t) \coloneqq t^{12} + t^6 + t^4 + 2t^3 + t$ gilt

$$g'(t) = 4t^3 + 1 = t^3 + 1 = (t+1)^3\,.$$

Da -1 eine Nullstelle von $g(t)$ ist, ist somit -1 die einzige gemeinsame Nullstelle des Polynoms $g(t)$.

Aufgabe 4

(a)

Wir bestimmen zunächst, wieviele $z \in K$ von der Form $z = x^2$ für passendes $x \in K$ ist, d.h. wie viele Zahlen aus K bereits Quadratzahlen sind. Da $0^2 = 0$ gilt, genügt es hierfür, die Elemente $z \in K \smallsetminus \{0\} = K^\times$ zu betrachten.

Die Abbildung

$$q\colon K^\times \to K^\times\,, \quad x \mapsto x^2$$

ist ein Gruppenhomomorphismus mit

$$\ker q = \{x \in K^\times \mid x^2 = 1\} = \{1, -1\}$$

(denn dies sind genau die Nullstellen des Polynoms $t^2 - 1 = (t+1)(t-1) \in K[t]$).

1. Gilt $\mathrm{char}(K) = 2$, so gilt $1 = -1$, so dass $\ker q = 1$ gilt. In diesem Fall ist q injektiv, und wegen der Endlichkeit von q somit bereits bijektiv. Also ist dann jedes $z \in K^\times$ ein Quadrat.

2. Gilt $\mathrm{char}(K) \neq 2$, so gilt $1 \neq -1$, und somit $|\ker q| = 2$. Dann gilt

$$|\mathrm{im}\, q| = \frac{|K^\times|}{|\ker q|} = \frac{|K| - 1}{2} \,.$$

   Dann ist also genau die Hälfte aller $z \in K^\times$ ein Quadrat.

Im Fall $\mathrm{char}(K) = 2$ folgt mit $0^2 = 0$, dass jedes $z \in K$ ein Quadrat ist, die Abbildung $K \to K$, $x \mapsto x^2$ also bijektiv ist. Im Fall $\mathrm{char}(K) \neq 2$ folgt mit $0^2 = 0$ hingegen, dass

$$|\{x^2 \mid x \in K\}| = 1 + |\{x^2 \mid x \in K^\times\}| = 1 + \frac{|K| - 1}{2} = \frac{|K| + 1}{2} \,.$$

Da $a \in K^\times$ gilt, ist die Abbildung $K \to K$, $z \mapsto az$ bijektiv, und somit

$$|\{ax^2 \mid x \in K\}| = |\{x^2 \mid x \in K\}| = \begin{cases} |K| & \text{falls } \mathrm{char}(K) = 2\,, \\ (|K| + 1)/2 & \text{falls } \mathrm{char}(K) \neq 2\,. \end{cases}$$

(c)

Es gilt $\mathrm{char}(K) = 2$, da $|K|$ gerade ist. Wie bereits gesehen ist die Abbildung $K \to K$, $x \mapsto ax^2$ deshalb bijektiv. Also ist auch die Abbildung $K \to K$, $x \mapsto 1 + ax^2$ bijektiv. Es gibt also für jedes $z \in K$ ein eindeutiges Element $x \in K$ mit $z = 1 + ax^2$.

(b)

Gilt $\mathrm{char}(K) = 2$, ist also $|K|$ gerade, so lässt sogar noch $y = 0$ wählen, wie bereits gezeigt. Es bleibt also nur noch der Fall $\mathrm{char}(K) \neq 2$ zu betrachten. Wie bereits gesehen, gelten dann

$$|\{1 + ax^2 \mid x \in K\}| = |\{ax^2 \mid x \in K\}| = |\{x^2 \mid x \in K\}| = \frac{|K| + 1}{2}$$

und

$$|\{-by^2 \mid y \in K\}| = |\{y^2 \mid y \in K\}| = |\{y^2 \mid y \in K\}| = \frac{|K| + 1}{2} \,.$$

Dabei gilt

$$\frac{|K| + 1}{2} + \frac{|K| + 1}{2} = |K| + 1 > |K| \,,$$

weshalb nach dem Schubfachprinzip

$$\{1 + ax^2 \mid x \in K\} \cap \{-by^2 \mid y \in K\} \neq \emptyset$$

gilt. Es gibt also $x, y \in K$ mit $1 + ax^2 = -by^2$, also mit $1 + ax^2 + by^2 = 0$.