Anmerkungen und Lösungen zu

Einführung in die Algebra

Blatt 11

Jendrik Stelzner

Letzte Änderung: 23. 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 (da $\mathbb{Q}(\sqrt[4]{2})$ ein Unterkörper von $\mathbb{R}$ ist). Es gibt deshalb keinen Körperhomomorphismus $\hat{f}\colon \mathbb{Q}(\sqrt[4]{2}) \to \mathbb{Q}(\sqrt[4]{2})$ mit $\hat{f}(\sqrt{2}) = -\sqrt{2}$. Deshälb 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 kann $f(t) = t$ gewählt werden, und gilt $S \neq \emptyset$, so lässt sich $f(t) = 1 + \prod_{s \in S}(t - s)$ wählen.

(d)

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

(e)

Die Aussage ist *wahr*: Ist K ein endlicher Integritätsbereich, so ist K per Definition kommutativ, und es gilt $K \neq 0$. Es bleibt daher nur noch 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 $1 = \lambda_x(y) = xy$, weshalb x eine Einheit in K ist.

Bemerkung 1. Ist $D \neq 0$ ein (nicht notwendigerweise kommutativer) links- und rechtsnullteilerfreier endlicher 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 (man mache sich bewusst, 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. Die Kommutativität von K muss in dieser Aufgabe deshalb nicht vorausgesetzt werden.

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 deshalb

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

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 der Körperhomomorphismus f 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. Hiermit 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 nach dem vorherigen Aufgabenteil

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

(c)

Hat $f(t)$ keine 9 verschiedenen Nullstellen in K, so hat $f(t)$ im im algebraischen Abschluss $\overline{\mathbb{F}_3} \supseteq K$ 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

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

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

- 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 $f'(t)$ 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 von $f(t)$.

(ii)

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 auch eine Nullstelle von $g(t)$ ist, handelt es sich bei -1 um die einzige mehrfache Nullstelle von $g(t)$.

Aufgabe 4

(a)

Wir bestimmen zunächst, wieviele $z \in K$ von der Form $z = x^2$ für passendes $x \in K$ sind, d.h. wie viele Zahlen $z \in K$ bereits Quadratzahlen sind. Dabei genügt es im Folgenden, die Elemente $z \in K \setminus \{0\} = K^\times$ zu betrachten, da $0^2 = 0$ gilt.

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

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

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

Im Fall $\operatorname{char}(K) = 2$ 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. (Man bemerke, dass dies genau der Frobenius-Automorphismus ist.) Im Fall $\operatorname{char}(K) \neq 2$ 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

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

(c)

Es gilt $\operatorname{char}(K) = 2$, 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 $\operatorname{char}(K) = 2$, ist also $|K|$ gerade, so haben wir bereits gezeigt, dass sich sogar noch $y = 0$ wählen lässt. Es bleibt also nur noch der Fall $\operatorname{char}(K) \neq 2$ 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

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

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 $1 + ax^2 + by^2 = 0$.

Aufgabe 6

(a)

Die in dieser Aufgabe gezeigte Aussage, dass jede endliche abelsche Gruppe A zu einem direkten Produkt von zyklischen p-Gruppen isomorph ist (wobei p die Primfaktoren der Ordnung $|A|$ durchläuft), verallgemeinert sich zum *Fundamentalsatz über endlich erzeugte abelsche Gruppen.*

Satz 2 (Fundamentalsatz über endlich erzeugte abelsche Gruppen)**.** *Ist A eine endlich erzeugte abelsche Gruppe, so gilt*

$$A \cong \mathbb{Z}^r \times \prod_{i=1}^{s} (\mathbb{Z}/p_i^{\nu_i})$$

mit $r, s \geq 0$, $\nu_1, \ldots, \nu_s \geq 1$ und $p_1, \ldots, p_s$ prim. Dabei sind die Zahlen r, s eindeutig, und die Paare $(p_1, \nu_1), \ldots, (p_s, \nu_s)$ eindeutig bis auf Permutation.

Ist A eine endliche abelsche Gruppe, so muss $r = 0$ gelten, und wir erhalten die Aussage der Aufgabe. Wir erhalten sogar noch eine Eindeutigkeitsaussage (bis auf Permutation der Faktoren).

Bemerkung 3. In der Praxis stellt sich häufig die Frage, wie für gegebene Elemente $a_1, \ldots, a_m \in \mathbb{Z}^n$ die Gruppe

$$A \coloneqq \mathbb{Z}^n / \langle a_1, \ldots, a_m \rangle$$

aussieht. Da $\mathbb{Z}^n$ als abelsche Gruppe von den (endlich vielen) Standardbasisvektoren $e_1, \ldots, e_n \in \mathbb{Z}^n$ erzeugt wird, ist auch A endlich erzeugt. Nach Satz 2 gilt deshalb

$$A \cong \mathbb{Z}^r \times \prod_{i=1}^{s} (\mathbb{Z}/p_i^{\nu_i}) \,.$$

Es gibt nun einen Algorithmus, um die rechte Seite zu berechnen.

1. Man trage zunächst die $a_1, \ldots, a_n$ als Spalten in eine Matrix $A \in \mathrm{M}(m \times n, \mathbb{Z})$ ein.
2. Durch elementare Zeilen- und Spaltenumformungen (wobei man beim Skalieren der Zeilen und Spalten nur die Einheiten $\pm 1 \in \mathbb{Z}$ nutzen darf) bringe man A in eine (2×2)-Blockgestalt

$$D = \left(\begin{array}{ccc|c} d_1 & & & 0 \\ & \ddots & & \vdots \\ & & d_s & 0 \\ \hline 0 & \cdots & 0 & 0 \end{array}\right),$$

   mit $d_1, \ldots, d_s \geq 1$.

3. Es gilt dann
$$A \cong \mathbb{Z}^{m-s} \times (\mathbb{Z}/d_1) \times \cdots \times (\mathbb{Z}/d_s)\,.$$
Mithilfe des chinesischen Restklassensatzes lassen sich dann die Faktoren $\mathbb{Z}/d_i$ noch weiter in direkte Produkte von zyklischen p-Gruppen zerlegen.

Insbesondere lassen sich der Fundamentalsatz über endlich erzeugte abelsche Gruppen (inklusive der von uns gezeigten Aussagen über endliche abelsche Gruppen) auch rein algorithmisch begründen. (Zumindest die Existenz der entsprechenden Zerlegungen.)

Bemerkung 4. Der Fundamentalsatz über endlich erzeugte abelsche Gruppen verallgemeinert sich weiter zum *Fundamentalsatz über endlich erzeugte Moduln über Hauptidealringen* (den wir hier nicht angeben werden). Für den Hauptidealring $\mathbb{Z}$ erhält man hieraus den Fundamentalsatz über endlich erzeugte abelsche Gruppen; für den Hauptidealring $K[t]$, wobei K ein algebraisch abgeschlossener Körper ist, erhält man (unter anderem) die Jordan-Normalform aus der linearen Algebra.

Insbesondere lassen sich die Beweise zu Aufgaben 5 und 6 in einen Beweis für die Existenz der Jordan-Normalform über algebraisch abgeschlossenen Körpern umschreiben. (Die Zerlegung einer endlichen abelschen Gruppe in ihre p-Sylowuntergruppen wird dabei durch die Zerlegung eines endlichdimensionalen Vektorraums in die verallgemeinerten Eigenräume, bzw. Haupträume ersetzt.) Hieraus ergibt sich auch, dass die Lösungen zu Aufgabe 5 nicht sehr viel besser als die Beweise für die Existenz der Jordan-Normalform seien können.

(b)

Ein *Partition* einer Menge X ist eine Kollektion von nicht-leeren Teilmenge $\mathcal{Y} \subseteq \mathcal{P}(X)$ mit $X = \bigcup_{Y \in \mathcal{Y}} Y$ und $Y_1 \cap Y_2 = \emptyset$ für alle $Y_1, Y_2 \in \mathcal{Y}$. Partitionen von X entsprechen also den Möglichkeiten, die Menge X in paarweise disjunkte, nicht-leere Teilmengen zu zerlegen. Für alle $n \geq 1$ sei $P(n)$ die Anzahl der Partitionen einer n-elementigen Menge. (Es gelten etwa $P(1) = 1$, $P(2) = 2$, $P(3) = 5$ und $P(4) = 15$.)

Es sei nun $N \geq 1$ mit Primfaktorzerlegung $N = p_1 \cdots p_n$. Dann liefert jede Partition $\{1, \ldots, n\} = A_1 \cup \cdots \cup A_r$ in paarweise disjunkte Teilmengen $A_1, \ldots, A_r \subseteq \{1, \ldots, n\}$ eine endliche abelsche Gruppe
$$\mathbb{Z} \Big/ \left(\prod_{p \in A_1} p \right) \times \cdots \times \mathbb{Z} \Big/ \left(\prod_{p \in A_r} p \right)$$
der Ordnung N. Nach den vorherigen Ergebnissen ist jede abelsche Gruppe der Ordnung N isomorph zu einer Gruppe dieser Form. Es genügt daher zu zeigen, dass
$$P(n) \leq n^n$$
für alle $n \geq 1$ gilt. Wir zeigen dies per Induktion über n:

Für $n = 1$ gilt $P(n) = 1 = 1^1 = n^n$. Es sei nun $n \geq 2$ und es gelte $P(m) \leq m^m$ für alle $m = 1, \ldots, n-1$. Um $P(n)$ entsprechend abzuschätzen, betrachten wir alle

Teilmengen $A \subseteq \{1, \dots, n\}$, die 1 enthalten. Für jedes $k \geq 1$ gibt es genau $\binom{n-1}{k-1}$ viele k-elementige solche Teilmengen. Für jede solche Menge gibt es dann $P(n-k)$ viele Partitionen für das Komplement $\{1, \dots, n\} \setminus A$, also Möglichkeiten, dieses Komplement weiter disjunkt zu zerlegen. Wir erhalten somit, dass

$$\begin{aligned} P(n) &= \sum_{k=1}^{n} \binom{n-1}{k-1} P(n-k) = \sum_{k=0}^{n-1} \binom{n-1}{k} P(n-k-1) \\ &\leq \sum_{k=0}^{n-1} \binom{n-1}{k} (n-k-1)^{(n-k-1)} \leq \sum_{k=0}^{n-1} \binom{n-1}{k} (n-1)^{(n-1-k)} \cdot 1^k \\ &= (n-1+1)^{n-1} = n^{(n-1)} \leq n^n \,. \end{aligned}$$

Aufgabe 7

Lemma 5. *Es sei p prim, und es seien $n, m \geq 1$. Dann gibt es genau dann eine Einbettung $\mathbb{F}_{p^n} \hookrightarrow \mathbb{F}_{p^m}$, also einen Körperhomomorphismus $\mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$, wenn $n \mid m$ gilt.*

Beweis. Falls es eine Einbettung $\mathbb{F}_{p^n} \hookrightarrow \mathbb{F}_{p^m}$ gibt, so können wir o.B.d.A. den Körper $\mathbb{F}_{p^n}$ als einen Unterkörper von $\mathbb{F}_{p^m}$ auffassen. Nach der Multiplikativität des Grades gilt dann

$$m = [\mathbb{F}_{p^m} : \mathbb{F}_p] = [\mathbb{F}_{p^m} : \mathbb{F}_{p^n}][\mathbb{F}_{p^n} : \mathbb{F}_p] = [\mathbb{F}_{p^m} : \mathbb{F}_{p^n}] \cdot n \,,$$

und somit $n \mid m$. Gilt andererseits $n \mid m$, so lässt sich auf verschiedene Weisen vorgehen:

- Das Polynom $t^{p^n} - t$ ein Teiler des Polynoms $t^{p^m} - t$. Dies lässt sich auf verschiedene Weisen sehen:
  - Ist $\overline{\mathbb{F}_p}$ ein algebraischer Abschluss von $\mathbb{F}_p$, so zerfallen beide Polynome über $\overline{\mathbb{F}_p}$ in paarweise verschieden Linearfaktoren (denn beide Polynome sind separabel). Für jede Nullstelle $x \in \overline{\mathbb{F}_p}$ von $t^{p^n} - t$ gilt $x^{p^n} = x$. Dann gilt auch $x^{p^m} = x$, da m ein Vielfaches von n ist (und somit die Abbildung $y \mapsto y^{p^m}$ durch (m/n)-faches Anwenden der Abbildung $y \mapsto y^{p^n}$ gegeben ist). Also ist jeder Linearfaktor von $t^{p^n} - t$ auch ein Linearfaktor von $t^{p^m} - t$.
  - Indem wir beide Polynome durch t teilen, genügt es $(t^{(p^n-1)} - 1) \mid (t^{(p^m-1)} - 1)$ zu zeigen.
    Behauptung. *Es sei R ein Ring und es seien $a \in R$, $k \geq 1$. Dann gilt $(a-1) \mid (a^k - 1)$.*

    Beweis. Es gilt $a^k - 1 = (a-1)(a^{k-1} + a^{k-2} + \cdots + 1)$. □

    Nach der Behauptung genügt es zu zeigen, dass $(p^n - 1) \mid (p^m - 1)$ gilt, denn dann ist $t^{(p^m-1)}$ eine Potenz von $t^{(p^n-1)}$. Durch erneutes Anwenden der Behauptung genügt es hierfür zu zeigen, dass p^m eine Potenz von p^n ist. Dies ergibt sich aus $n \mid m$.

Da $\mathbb{F}_{p^m}$ ein Zerfällungkörper des Polynoms $t^{p^m} - t$ ist, folgt damit, dass $\mathbb{F}_{p^m}$ einen Zerfällungskörper des Polynoms $t^{p^n} - t$, also $\mathbb{F}_{p^n}$ enthält.

Zum besseren Verständnis der zu zeigenden Aussage möchten wir auch die folgende Argumentation angeben, die zur Abgabe des Übungszetteln noch nicht zur Verfügung stand:

- Die Erweiterung $\mathbb{F}_{p^m}/\mathbb{F}_p$ ist galoissch mit Galoisgruppe $\mathrm{Gal}\,(\mathbb{F}_{p^m}/\mathbb{F}_p) \cong \mathbb{Z}/m$. Da $n \mid m$ gilt, enthält $\mathrm{Gal}\,(\mathbb{F}_{p^m}/\mathbb{F}_p)$ somit eine Untergruppe $G \leq \mathrm{Gal}\,(\mathbb{F}_{p^m}/\mathbb{F}_p)$ der Ordnung m/n. Nach dem Hauptsatz der Galoistheorie gilt für den zugehörigen Fixkörper $K \coloneqq (\mathbb{F}_{p^m})^G$, dass die Körpererweiterung $\mathbb{F}_{p^m}/K$ galoissch mit Galoisgruppe $\mathrm{Gal}\,(\mathbb{F}_{p^m}/K) = G$ ist, und (somit) den Grad $[\mathbb{F}_{p^m} : K] = |G| = m/n$ hat. Nach der Multiplikativität des Grades gilt nun

$$m = [\mathbb{F}_{p^m} : \mathbb{F}_p] = [\mathbb{F}_{p^m} : K][K : \mathbb{F}_p] = \frac{m}{n} \cdot [K : \mathbb{F}_p]\,,$$

  und somit $[K : \mathbb{F}_p] = n$. Nach der Klassifikation endlicher Körper gilt für den Unterkörper $K \subseteq \mathbb{F}_{p^m}$ deshalb $K \cong \mathbb{F}_{p^n}$.

Mit ein wenig Abänderung der obigen Idee wird nicht der gesamte Hauptsatz der Galoistheorie benötigt. Es genügt bereits der Spezialfall der Galois-Korrespondenz für endliche Körper (Satz 19.1), der in der Vorlesung zum Zeitpunkt der Abgabe bereits bekannt war:

- Wie bereits gesehen, ist für jeden Unterkörper $K \subseteq \mathbb{F}_{p^m}$ der Grad $[K : \mathbb{F}_p]$ ein Teiler des Grades $[\mathbb{F}_{p^m} : \mathbb{F}_p] = m$. Dabei ist K durch den Grad $[K : \mathbb{F}_p] = d$ nach der Klassifikation endlicher Körper bereits eindeutig als

$$K = \left\{ x \in K \,\middle|\, x^{p^d} = x \right\}$$

  bestimmt. Es gibt also höchsten so viele Unterkörper $K \subseteq \mathbb{F}_{p^m}$, wie es positive Teiler $d \mid m$ gibt.

  Nach Satz 19.1 gibt eine 1:1-Korrespondenz

$$\{\text{Unterkörper } K \subseteq \mathbb{F}_{p^m}\} \overset{1:1}{\longleftrightarrow} \{\text{Untergruppen } G \leq \mathrm{Aut}(\mathbb{F}_{p^m})\}\,,$$

  wobei $\mathrm{Aut}(\mathbb{F}_{p^m}) = \langle \mathrm{Fr} \rangle \cong \mathbb{Z}/m$ gilt. Da $\mathbb{Z}/m$ für jeden positiven Teiler $d \mid m$ eine eindeutige Untergruppe der Ordnung d besitzt[1], enthält $\mathbb{F}_{p^m}$ tatsächlich schon so viele Unterkörper $K \subseteq \mathbb{F}_{p^m}$ wie es positive Teiler $d \mid m$ gibt.

  Zusammen erhalten wir somit, dass $\mathbb{F}_{p^m}$ für jeden positven Teiler $d \mid m$ einen Unterkörper $K \subseteq \mathbb{F}_{p^m}$ mit $[K : \mathbb{F}_p] = d$ besitzt. Inbesondere gilt dies für $d = n$. □

[1] Die vorherige Argumenation zeigt, dass es für einen positiven Teiler $d \mid m$ eigentlich natürlicher ist, die eindeutige Untergruppe von Ordnung m/d zu betrachten. Es geht es uns in dieser Argumentation aber nur um die Anzahl der Untergruppen, weshalb wir auch die hier genutzte Formulierung wählen können.