C. Dietzel, M. Künzer

Algebra für Lehramt, SoSe 20

Lösung 11

Aufgabe 41 Sei K ein endlicher Körper. Wir schreiben $q := |K|$.

(1) Man zeige, daß q eine Potenz einer Primzahl ist.

(2) Man bestimme x^{q-1} für $x \in K^\times$.

(3) Man bestimme $x^q - x + 1$ für $x \in K$.

(4) Ist K algebraisch abgeschlossen?

Lösung zu Aufgabe 41:

(1) Der kanonische Ringhomomorphismus $\varphi : \mathbb{Z} \to \mathbb{F}_q$ ist aufgrund der Endlichkeit von $\mathbb{F}_q$ nicht injektiv; folglich ist $p := \mathrm{char}(\mathbb{F}_q) > 0$.

Ließe sich p nun schreiben als $k_1 \cdot k_2$ mit $k_1, k_2 \in \mathbb{Z}_{\geqslant 2}$, so wären $\varphi(k_1), \varphi(k_2) \neq 0$, aber $\varphi(k_1) \cdot \varphi(k_2) = \varphi(k_1 k_2) = \varphi(p) = 0$. Dies ist in einem Körper nicht möglich, somit muss p prim sein.

Vermöge des injektiven Homomorphismus $\overline{\varphi} : \mathbb{Z}/(p) \to \mathbb{F}_q$ enthält $\mathbb{F}_q$ also den Unterkörper $\mathbb{F}_p = \mathbb{Z}/(p)$ und kann insbesondere als $\mathbb{F}_p$-Vektorraum aufgefasst werden.

Da $\mathbb{F}_q$ endlich ist, muss auch $[\mathbb{F}_q : \mathbb{F}_p] = \dim_{\mathbb{F}_p} \mathbb{F}_q$ endlich sein. Damit ist

$$|\mathbb{F}_q| = |\mathbb{F}_p|^{\dim_{\mathbb{F}_p} \mathbb{F}_q} = p^{[\mathbb{F}_q : \mathbb{F}_p]}.$$

(2) Vermöge der Multiplikation in K ist $K^\times$ eine Gruppe mit $|K^\times| = |K| - 1 = q - 1$. Nach Korollar 88 ist für alle $x \in K^\times$ also

$$x^{q-1} = x^{|K^\times|} = 1.$$

(3) Ist $x \in K^\times$, so impliziert Teil (2) dieser Aufgabe, dass

$$x^q = x \cdot x^{q-1} = x \cdot 1 = x.$$

Ist $x = 0$, so ist $x^q = 0^q = 0$. Folglich ist $x^q = x$ für alle $x \in K$.

Das impliziert für alle $x \in K$, dass

$$x^q - x + 1 = x - x + 1 = 1$$

ist.

(4) Nach Teil (3) nimmt das Polynom $X^q - X + 1 \in \mathbb{F}_q[X]$ ausschließlich den Wert 1 an, besitzt also keine Nullstellen. Wäre $\mathbb{F}_q$ algebraisch abgeschlossen, hätte es zumindest eine Nullstelle in $\mathbb{F}_q$. Demnach ist $\mathbb{F}_q$ nicht algebraisch abgeschlossen.

Aufgabe 42 Sei K ein Körper. Sei V ein K-Vektorraum.
Sei $X \subseteq V$ eine Teilmenge, nicht notwendig endlich.
Eine *Linearkombination* in X ist ein Element der Form $\sum_{i\in[1,n]} \lambda_i x_i \in V$, wobei $n \geqslant 0$, wobei $x_i \in X$ für $i \in [1,n]$, wobei $x_i \neq x_j$ für $i, j \in [1,n]$ mit $i \neq j$ und wobei $\lambda_i \in K$ für $i \in [1,n]$.
Eine solche Linearkombination heißt *nichttrivial*, falls es ein $i \in [1,n]$ gibt mit $\lambda_i \neq 0$.
Es heißt X *linear unabhängig*, wenn jede nichttriviale Linearkombination in X ungleich 0 ist.
Es heißt X *erzeugend*, wenn jedes Element von V eine Linearkombination in X ist.
Es heißt X eine *Basis* von V, wenn X linear unabhängig und erzeugend ist.

(1) Seien $Y \subseteq Z \subseteq V$ gegeben mit Y linear unabhängig und mit Z erzeugend.
Sei $\mathcal{U} := \{\, X \,:\, \text{es ist } Y \subseteq X \subseteq Z \text{ und } X \text{ linear unabhängig} \,\}$. Es ist $\mathcal{U} = (\mathcal{U}, \subseteq)$ ein Poset.
Man zeige, daß in $\mathcal{U}$ jede Kette eine obere Schranke besitzt.

(2) Man zeige, daß es in $\mathcal{U}$ ein maximales Element gibt und daß dies eine Basis von V ist.

Lösung zu Aufgabe 42:

(1) Wir stellen zunächst fest, dass eine Teilmenge $X \subseteq V$ genau dann unabhängig ist, wenn für paarweise verschiedene $x_i \in V$ ($i \in [1,n]$, $n \geqslant 0$) sowie Elemente $\lambda_i \in K$ ($i \in [1,n]$) stets die nachfolgende Implikation gilt:

$$\sum_{i\in[1,n]} \lambda_i x_i = 0 \quad \Rightarrow \quad \lambda_1 = \lambda_2 = \ldots = \lambda_n = 0.$$

Mit dieser äquivalenten Formulierung werden wir nachfolgend arbeiten.

Sei nun $C \in \mathrm{Chain}(\mathcal{U})$.

Ist $C = \emptyset$, so ist bereits Y eine obere Schranke von C. Wir dürfen also annehmen, dass $C \neq \emptyset$ ist.

Wir werden nun zeigen, dass $A := \bigcup C \in \mathcal{U}$ ist:

Da $X \subseteq Z$ für alle $X \in C$, ist auch $A = \bigcup C \subseteq Z$.

Da zudem $Y \subseteq X$ für $X \in C$, so ist auch $Y \subseteq \bigcup C = A$.

Wir haben die lineare Unabhängigkeit von A zu zeigen.

Seien dazu $x_1, \ldots, x_n \in A$ ($n \geqslant 0$), wobei die Elemente x_i ($i \in [1,n]$) paarweise verschieden seien. Seien außerdem $\lambda_1, \ldots, \lambda_n \in K$ so gegeben, dass

$$(*) \qquad \sum_{i\in[1,n]} \lambda_i x_i = 0$$

ist. Dann gibt es $X_1, \ldots, X_n \in C$, sodass jeweils $x_i \in X_i$ ist für $i \in [1,n]$. Wir dürfen ohne Einschränkung annehmen, dass

$$X_1 \subseteq X_2 \subseteq \ldots \subseteq X_n.$$

Dann ist für alle $i \in [1,n]$ das Element $x_i \in X_i \subseteq X_n$. Da damit $x_1, \ldots, x_n \in X_n$ sind und X_n eine linear unabhängige Teilmenge von V ist, impliziert $(*)$, dass $\lambda_i = 0$ ist für $i \in [1,n]$. Also ist A auch linear unabhängig.

Wir schließen, dass $A = \bigcup C \in \mathcal{U}$ ist. Da für alle $X \in C$ auch $X \subseteq A$ gilt, ist A eine obere Schranke für die Kette C.

(2) Wir haben in Teil (1) der Aufgabe gezeigt, dass jede Kette eine obere Schranke besitzt. Nach Zorns Lemma (Lemma 239) gibt es ein maximales Element $X \in \mathcal{U}$.

Es ist $Y \subseteq X \subseteq Z$.

Wir zeigen nun, dass X eine Basis ist:

Die Menge X ist als Element von $\mathcal{U}$ linear unabhängig.

Wir *nehmen* nun *an*, X ist nicht erzeugend.

Da Z erzeugend ist, ist jedes Element in V eine Linearkombination in Z. Dank Annahme können wir ein $z \in Z$ wählen, das nicht im K-linearen Erzeugnis von X liegt. Insbesondere ist $z \notin X$.

Wir zeigen, dass dann $X' := X \cup \{z\}$ eine linear unabhängige Menge mit $Y \subseteq X' \subseteq Z$ ist. Seien dazu paarweise verschiedene $x_i \in X$ ($i \in [1,n]$, $n \in \mathbb{Z}_{\geqslant 0}$) gegeben, sowie Elemente $\lambda_i \in K$ ($i \in [1,n]$) und $\mu \in K$ so, dass

$$\mu z + \sum_{i \in [1,n]} \lambda_i x_i = 0$$

ist.

Falls $\mu = 0$ ist, so ist $\sum_{i\in[1,n]} \lambda_i x_i = 0$, und aufgrund der linearen Unabhängigkeit von X ist $\lambda_i = 0$ für $i \in [1,n]$.

Ist $\mu \neq 0$, so gilt

$$\mu z = \sum_{i \in [1,n]} -\lambda_i x_i \quad \Rightarrow \quad z = \sum_{i \in [1,n]} -\frac{\lambda_i}{\mu} x_i \; .$$

Dies kann aber nicht sein, da wir angenommen haben, dass z *keine* Linearkombination in X ist. Dieser Fall tritt also nicht ein.

Es ist also $\mu = 0$ sowie $\lambda_i = 0$ für $i \in [1,n]$. Das beweist, dass X' linear unabhängig ist.

Es ist also $X' \in \mathcal{U}$. Weiterhin ist $X \subset X'$, im *Widerspruch* zur Maximalität von X.

Unsere Annahme war demnach falsch. Also muss X erzeugend sein.

Da X linear unabhängig und erzeugend ist, ist X eine Basis.

> Was impliziert diese Aufgabe für den Spezialfall, dass $Y \subseteq V$ linear unabhängig und $Z = V$ ist? Was impliziert sie für den Fall, dass $Y = \emptyset$ ist und $Z \subseteq V$ erzeugend?

Aufgabe 43 Sei K ein Körper. Sei $L|K$ ein algebraischer Abschluß.

(1) Man finde eine Abbildung $\varphi : L \to K[X]^\times$ mit $|\varphi^{-1}(f(X))| \leqslant \deg(f(X))$ für $f(X) \in K[X]^\times$.

(2) Sei $\mathrm{char}(K) = 0$. Sei $f(X) \in K[X]$ normiert und irreduzibel.
Man zeige $|\{\, y \in L \,:\, f(y) = 0 \,\}| = \deg(f(X))$.

(3) Sei K endlich. Sei $f(X) \in K[X]$ normiert und irreduzibel.
Man zeige $|\{\, y \in L \,:\, f(y) = 0 \,\}| = \deg(f(X))$.

Lösung zu Aufgabe 43:

(1) Wir definieren

$$\begin{aligned}\varphi : L &\to K[X]^\times \\ \alpha &\mapsto \mu_{\alpha,K}(X).\end{aligned}$$

Sei $f(X) \in K[X]^\times$ zu betrachten.

Ist $f(X)$ irreduzibel und normiert, so ist es ein Minimalpolynom jeder seiner Nullstellen in L.

Ist $f(X)$ nicht irreduzibel und normiert, dann kann es auch kein Minimalpolynom irgendeines Elements aus L.

Somit gilt:

$$\varphi^{-1}(f(X)) = \begin{cases}\{\alpha \in L : f(\alpha) = 0\} & \text{falls } f(X) \text{ irreduzibel und normiert} \\ \emptyset & \text{sonst}\end{cases}.$$

Für den Fall, dass $f(X) \in K[X]^\times$ normiert und irreduzibel ist, impliziert Bemerkung 205, dass

$$|\varphi^{-1}(f(X))| = |\{\alpha \in L : f(\alpha) = 0\}| \leqslant \deg(f(X))$$

gilt. In allen anderen Fällen ist $\varphi^{-1}(f(X)) = \emptyset$ und es ist

$$|\varphi^{-1}(f(X))| = 0 \leqslant \deg(f(X)).$$

In jedem Falle gilt also $|\varphi^{-1}(f(X))| \leqslant \deg(f(X))$.

(2) Wir setzen $n := \deg(f(X))$. Sei

$$f(X) = \prod_{i=1}^{n}(X - y_i)$$

die Zerlegung von $f(X)$ in Linearfaktoren in $L[X]$ mit $y_1, \ldots, y_n \in L$.

Offenbar ist $\{y_1, \ldots, y_n\} = \{y \in L : f(y) = 0\}$, demzufolge ist die zu beweisende Aussage äquivalent zu $|\{y_1, \ldots, y_n\}| = n$; dies wiederum ist gleichbedeutend damit, dass $y_1, \ldots, y_n$ paarweise verschieden sind.

Wegen $\mathrm{char}(K) = 0$ und $\deg(f(X)) \geqslant 2$ ist $f'(X) \neq 0$. Da $0 \leqslant \deg(f'(X)) < n$ ist, gilt $f(X) \nmid f'(X)$, somit ist $\mathrm{ggT}(f(X), f'(X)) \neq f(X)$. Da $f(X)$ aufgrund seiner Irreduzibilität jedoch nur die normierten Teiler 1 und $f(X)$ besitzt, ist $\mathrm{ggT}(f(X), f'(X)) = 1$.

Nach Lemma 215.(1) ist $f(X)$ also quadratfrei. Somit sind die Linearfaktoren $X - y_i$ für $i \in [1, n]$ paarweise verschieden. Insbesondere sind die Elemente $y_1, \ldots, y_n$ paarweise verschieden, was zu beweisen war.

(3) Wie in Teil (2) sei $n := \deg(f(X))$ und

$$f(X) = \prod_{i=1}^{n}(X - y_i)$$

die Zerlegung von $f(X)$ in Linearfaktoren in $L[X]$, wobei $y_1, \ldots, y_n \in L$ sind. Weiterhin sei $|K| =: q = p^k$, wobei $p := \mathrm{char}(K)$.

Mit derselben Argumentation wie in Teil (2) kann die zu zeigende Aussage darauf zurückgeführt werden, dass die Elemente $y_1, \ldots, y_n$ paarweise verschieden sind.

Wir werden zuerst zeigen, dass $f'(X) \neq 0$ ist. Wir schreiben dafür

$$f(X) = \sum_{i=0}^{n} a_i X^i.$$

Dann ist

$$f'(X) = \sum_{i=0}^{n} i \cdot a_i X^i.$$

Annahme, es ist $f'(X) = 0$. Anhand dieser Darstellung erkennt man, dass dann für alle $i \in [0, n]$ gilt, dass $a_i = 0$ ist, falls $i \not\equiv_p 0$. Mit anderen Worten, nur die Koeffizienten können ungleich 0 sein, deren Index durch p teilbar ist. Insbesondere ist $n \equiv_p 0$.

Setzen wir $m := n/p$, so können wir $f(X)$ auch darstellen als

$$\begin{aligned} f(X) &= \sum_{j=0}^{m} a_{pj} X^{pj} \\ &= \sum_{j=0}^{m} a_{pj}^{q} X^{pj} \\ &= \sum_{j=0}^{m} (a_{pj}^{p^{k-1}})^p \cdot (X^j)^p \\ &= \left(\sum_{j=0}^{m} a_{pj}^{p^{k-1}} \cdot X^j \right)^p. \end{aligned}$$

Hierbei haben wir die für Aufgabe 41.(3) hergeleitete Identität $x^q = x$ für $x \in \mathbb{F}_q$ verwendet.

Wir haben eine Zerlegung von $f(X)$ gefunden, in der alle Faktoren Grad $m < n$ haben, im *Widerspruch* zur Irreduzibilität von $f(X)$.

Es ist also $f'(X) \neq 0$. Da damit $0 \leqslant \deg(f') < n$ ist, gilt $f(X) \nmid f'(X)$, und wir schließen aus der Irreduzibilität von $f(X)$, dass $\mathrm{ggT}(f(X), f'(X)) = 1$ ist. Folglich ist $f(X)$ quadratfrei.

In der gleichen Weise wie in Teil (2) folgt daraus die zu zeigende Aussage, dass die Elemente $y_1, \ldots, y_n$ paarweise verschieden sind.

Aufgabe 44 Sei X ein endliches Poset. Sei $x \in X$.
Man zeige die Äquivalenz der Aussagen (a) und (b).

(a) Es ist x ein terminales Element von X.

(b) Es ist x das einzige maximale Element von X.

Trifft diese Äquivalenz auch noch zu, wenn X nicht mehr als endlich vorausgesetzt wird?

Lösung zu Aufgabe 44:

(a) $\Rightarrow$ (b): Sei $x \in X$ terminal.

Wir zeigen, daß x maximal ist. *Annahme*, nicht. Dann gibt es ein Element $z \in X$ mit $x < z$. Da x terminal ist, ist $z \leqslant x$. Aus $z \leqslant x < z$ folgt $x = z$ und also $z < z$. Wir haben einen *Widerspruch*.

Sei nun auch $y \in X$ maximal. Da x terminal ist, gilt $y \leqslant x$. Aufgrund der Maximalität von y folgt daraus $x = y$.

Insgesamt ist demzufolge x das einzige maximale Element in X.

(b) $\Rightarrow$ (a): Sei x das einzige maximale Element in X.

Annahme, es ist x nicht terminal. Dann gibt es ein $y \in X$ mit $y \not\leqslant x$.

Wir setzen $y_1 := y$. Da y nicht maximal ist, können wir ein Element $y_2 \in X$ finden, sodass $y_1 < y_2$ ist. Es ist $y_2 \not\leqslant x$ – andernfalls wäre nämlich $y_1 < y_2 \leqslant x$, und damit $y_1 \leqslant x$.

Haben wir allgemeiner für ein $i \in \mathbb{N}$ das Element $y_i \in X$ konstruiert, welches $y_i \not\leqslant x$ erfüllt, so können wir stets ein Element $y_{i+1} \in X$ mit $y_i < y_{i+1}$ finden, für welches erneut $y_{i+1} \not\leqslant x$ gilt.

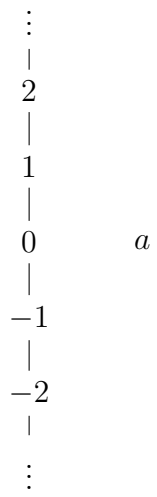
Auf diese Weise würden wir allerdings eine unendliche Kette $y_1 < y_2 < \dots$ erhalten, was der Endlichkeit von X widerspricht.

Ist X unendlich, so muss die Implikation (b) $\Rightarrow$ (a) nicht mehr gelten:

Wir setzen $X := \mathbb{Z} \sqcup \{a\}$ und versehen X mit der folgenden partiellen Ordnung:

$$x \leqslant_X y :\Leftrightarrow ((x = y) \vee ((x, y \in \mathbb{Z}) \wedge (x \leqslant_{\mathbb{Z}} y)))\,,$$

welche durch die rechts abgebildete Grafik veranschaulicht ist.
Nachfolgend werden wir $\leqslant_X$ durch $\leqslant$ bezeichnen und durch die Subindizierung $\leqslant_{\mathbb{Z}}$ die natürliche Ordnung auf $\mathbb{Z}$ von der auf X unterscheiden.



Wir überprüfen die Axiome für eine partielle Ordnung:

Reflexivität Per Definition gilt $x \leqslant x$.

Identitivität Für $x, y \in X$ gelte $x \leqslant y$ und $y \leqslant x$. Ist $x = a$, so muss auch $y = a$ sein und es folgt $x = y$. Ist $x \in \mathbb{Z}$, so ist auch $y \in \mathbb{Z}$ und es gilt $x \leqslant_{\mathbb{Z}} y$ sowie $y \leqslant_{\mathbb{Z}} x$, woraus ebenfalls $x = y$ folgt.

Transitivität Für $x, y, z \in X$ gelte $x \leqslant y$ und $y \leqslant z$. Ist $a \in \{x, y, z\}$, d.h. ist eines der Elemente x, y, z mit a identisch, so kann nur $x = y = z = a$ sein. Insbesondere ist dann $x = a \leqslant a = z$. Andernfalls sind $x, y, z \in \mathbb{Z}$ und es gilt $x \leqslant_{\mathbb{Z}} y$ sowie $y \leqslant_{\mathbb{Z}} z$. Es folgt $x \leqslant_{\mathbb{Z}} z$, woraus wiederum $x \leqslant z$ folgt.

Das einzige Element $x \in X$ mit $x \geqslant a$ ist $x = a$, somit ist a ein maximales Element in X. Es gibt kein weiteres maximales Element $x \in X$, denn ist $x \neq a$, so ist nämlich $x \in \mathbb{Z}$ und es ist $x < x + 1$. Folglich ist a das einzige maximale Element in X. Aber es ist a nicht terminal, da z.B. $1 \not\leqslant a$ ist.