Karlsruher Institut für Technologie

Institut für Algebra und Geometrie
Prof. Dr. Wilderich Tuschmann
Dr. Rafael Dahmen
Dr. Elisa Hartmann
Martin Günther, M. Sc.

Lineare Algebra I **Winter-Semester 2020/2021**

Musterlösung zu Übungsblatt 7 **21.12.20**

Aufgabe 1 (*ISBN-Nummern*) (*10 Punkte*)

Bücher wurden bis zum Jahr 2006 mit einer zehnstelligen ISBN-Nummer gekennzeichnet:

$$z_1{-}z_2\,z_3\,z_4{-}z_5\,z_6\,z_7\,z_8\,z_9{-}z_{10}.$$

Dabei kennzeichnet die erste Ziffer z_1 das Land, die Ziffern z_2, z_3, z_4 den Verlag, die Ziffern $z_5, \ldots, z_9$ das Buch, und die letzte Ziffer z_{10} ist eine Prüfziffer, für die auch die römische Zahl X (für 10) stehen kann. Die Prüfziffer wird dabei so berechnet, dass der Term

$$1z_1 + 2z_2 + 3z_3 + \ldots + 9z_9 + 10z_{10}$$

ein Vielfaches von 11 ist.

a) Bei der Eingabe der ISBN-Nummern werden häufig folgende Fehler gemacht:

   i) Genau eine der Ziffern wird falsch eingegeben, oder

   ii) Zwei beliebige der Ziffern werden vertauscht.

   Beweisen Sie: Wenn man einen dieser Fehler bei einer gültigen ISBN-Nummer macht, erhält man eine ISBN-Nummer mit falscher Prüfziffer.

b) Sie wollen ein Buch mit der ISBN-Nummer 0−465−02?85−0 bestellen. Eine Ziffer (?) können Sie nicht erkennen. Errechnen Sie diese Ziffer.

   Hinweis: Vielleicht brauchen Sie dabei: $7 \cdot 8 \equiv 1 \pmod{11}$.

c) Bei der neueren dreizehnstelligen ISBN-Nummer wird die Prüfziffer z_{13} so berechnet, dass der Term

$$z_1 + 3z_2 + z_3 + 3z_4 + \cdots + z_{11} + 3z_{12} + z_{13}$$

   durch 10 teilbar ist.

   Beweisen Sie: Die Vertauschung zweier benachbarter Ziffern z_i, z_{i+1} führt genau dann zu einer falschen Prüfziffer, falls die Differenz $z_i - z_{i+1}$ nicht durch 5 teilbar ist.

   Bemerkung: Die dreizehnstellige IBAN hat dieses schwächere Prüfverfahren, da sie mit den EAN-Nummern übereinstimmt, die weltweit für Barcodes verwendet werden. Beim Einlesen eines Barcodes ist ein Vertauschen von Ziffern sowieso sehr unwahrscheinlich.

Lösung zu Aufgabe 1

a) i) Angenommen, wir geben an der i-ten Stelle die Ziffer $\tilde{z}_i$ statt z_i ein und der neue Prüfterm ist immer noch durch 11 teilbar. Dann ist auch die Differenz $i(\tilde{z}_i - z_i)$ des neuen und alten Prüfterms durch 11 teilbar. Da 11 prim ist, muss 11 also i oder $\tilde{z}_i - z_i$ teilen.

Die Zahl i liegt zwischen 1 und 10 und kann somit nicht durch 11 teilbar sein. Da die Ziffern zwischen 0 und 10 liegen, liegt die Differenz $\tilde{z}_i - z_i$ zwischen -10 und 10, ist also nur dann durch 11 teilbar, wenn $\tilde{z}_i - z_i = 0$ gilt, wir also gar keinen Fehler gemacht haben.

ii) Vertauschen wir die i-te und j-te Ziffer und lassen alle anderen Ziffern gleich, beträgt die Differenz des neuen und alten Prüfterms $(jz_i + iz_j) - (iz_i + jz_j) = (z_i - z_j)(j - i)$. Wie oben begründet, liegt $(z_i - z_j)$ zwischen -10 und 10, dasselbe gilt für $i - j$. Die Differenz der beiden Prüferme kann also nur dann durch 11 teilbar sein, wenn $z_i = z_j$ oder $i = j$ gelten. In beiden Fällen hätten wir aber gar keinen Fehler gemacht.

b) Der Prüfterm ist genau dann durch 11 teilbar, wenn er das Null-Element im Ring $\mathbb{Z}/11\mathbb{Z}$ repräsentiert. In $\mathbb{Z}/11\mathbb{Z}$ gilt also

$$\begin{aligned}
& \sum_{i=1}^{10} i\, z_i \equiv 0 && \pmod{11} \\
\iff \quad & 7z_7 \equiv -\sum_{\substack{i=1 \\ i\neq 7}}^{10} i\, z_i && \pmod{11} \\
\iff \quad & z_7 \equiv 8 \cdot 7z_7 \equiv -8 \cdot \sum_{\substack{i=1 \\ i\neq 7}}^{10} i\, z_i && \pmod{11} \\
\iff \quad & z_7 \equiv -(2 \cdot 4 + 3 \cdot 6 + 4 \cdot 5 + 6 \cdot 2 + 8 \cdot 8 + 9 \cdot 5) && \pmod{11} \\
\iff \quad & z_7 \equiv -8(8 - 4 - 2 + 1 - 2 + 1) && \pmod{11} \\
\iff \quad & z_7 \equiv -8 \cdot 2 \equiv 6 && \pmod{11}
\end{aligned}$$

Also muss $z_7 = 6$ gelten und wir erhalten die ISBN-Nummer 0−465−02685−0.

c) Von zwei benachbarten Ziffern wird immer eine mit 1 und eine mit 3 multipliziert. Die Differenz der beiden Prüferme, wenn wir z_i und z_{i+1} vertauschen, beträgt also $\pm(z_i - z_j)(3 - 1) = \pm 2(z_i - z_j)$. Diese ist nur dann durch 10 teilbar, wenn $z_i - z_j$ durch 5 teilbar ist, also $z_i - z_j = \pm 5$ gilt, oder $z_i - z_j = 0$.

Aufgabe 2 (*10 Punkte*)

a) Gemäß Beispiel 4.1.3.(i) ist der Körper $\mathbb{Q}(\sqrt{2})$ aus Aufgabe 3 von Blatt 5 ein Vektorraum über $\mathbb{Q}$.

Beweisen Sie, dass die folgende Abbildung linear ist und bestimmen Sie eine Basis ihres Kerns:

$$\begin{aligned}
\varphi_1 \colon \mathbb{Q}^2 &\to \mathbb{Q}(\sqrt{2}) \\
\begin{pmatrix} a \\ b \end{pmatrix} &\mapsto \sqrt{2}\, a + \frac{b}{\sqrt{2}}
\end{aligned}$$

b) Zeigen Sie, dass die folgende Abbildung linear ist und bestimmen Sie eine Basis ihres Kerns:

$$\begin{aligned}\varphi_2 \colon \mathbb{F}_5^3 &\to \mathbb{F}_5^3 \\ \begin{pmatrix} a \\ b \\ c \end{pmatrix} &\mapsto \begin{pmatrix} a+2b+2c \\ 2a+3b+c \\ a+c \end{pmatrix}\end{aligned}$$

Lösung zu Aufgabe 2

a) Wir zeigen, dass $\mathbb{Q}(\sqrt{2})$ eine Körpererweiterung von $\mathbb{Q}$ ist. Die Teilmenge $\mathbb{Q}$ ist ein Unterkörper, denn $(\mathbb{Q}, +)$ ist eine Untergruppe, das Element $1 \in \mathbb{Q}$ und $\mathbb{Q}$ ist multiplikativ abgeschlossen. Nach Aufgabe 3 dieses Übungsblattes ist $\mathbb{Q}(\sqrt{2})$ ein Vektorraum über $\mathbb{Q}$.

Nun zeigen wir, dass φ_1 eine lineare Abbildung ist. Das Bild von φ ist tatsächlich in $\mathbb{Q}(\sqrt{2})$ enthalten, denn $\frac{1}{\sqrt{2}} = \sqrt{2}/2$. Seien $a, b, c, d \in \mathbb{Q}$. Dann ist

$$\begin{aligned}\varphi_1\left(\begin{pmatrix} a \\ b \end{pmatrix} + \begin{pmatrix} c \\ d \end{pmatrix}\right) &= \varphi_1\left(\begin{pmatrix} a+c \\ b+d \end{pmatrix}\right) \\ &= \sqrt{2}(a+c) + \frac{\sqrt{2}}{2}(b+d) \\ &= \sqrt{2}a + \frac{\sqrt{2}}{2}b + \sqrt{2}c + \frac{\sqrt{2}}{2}d \\ &= \varphi_1\left(\begin{pmatrix} a \\ b \end{pmatrix}\right) + \varphi_1\left(\begin{pmatrix} c \\ d \end{pmatrix}\right).\end{aligned}$$

Sei weiterhin $\lambda \in \mathbb{Q}$. Dann ist

$$\varphi_1\left(\lambda \begin{pmatrix} a \\ b \end{pmatrix}\right) = \varphi_1\left(\begin{pmatrix} \lambda a \\ \lambda b \end{pmatrix}\right) = \sqrt{2}\lambda a + \frac{\sqrt{2}}{2}\lambda b = \lambda(\sqrt{2}a + \frac{\sqrt{2}}{2}b) = \lambda\varphi_1\left(\begin{pmatrix} a \\ b \end{pmatrix}\right).$$

Nun bestimmen wir den Kern von φ_1. Eine Möglichkeit ist, eine Basis von $\mathbb{Q}(\sqrt{2})$ zu bestimmen und eine Basis von $\mathbb{Q}^2$ festzulegen und dann die entsprechende Matrix entlang der Basen zu bestimmen. In diesem Fall geht es durch draufschauen einfacher:

$$\begin{aligned}\ker \varphi_1 &= \left\{ \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{Q}^2 \mid \varphi_1\left(\begin{pmatrix} a \\ b \end{pmatrix}\right) = 0 \right\} \\ &= \left\{ \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{Q}^2 \mid \sqrt{2}a + \frac{\sqrt{2}}{2}b = 0 \right\} \\ &= \left\{ \begin{pmatrix} -t/2 \\ t \end{pmatrix} \in \mathbb{Q}^2 \mid t \in \mathbb{Q} \right\} \\ &= \mathrm{LH}\left(\begin{pmatrix} -1/2 \\ 1 \end{pmatrix}\right)\end{aligned}$$

b) Definiere die Matrix $A \coloneqq \begin{pmatrix} 1 & 2 & 2 \\ 2 & 3 & 1 \\ 1 & 0 & 1 \end{pmatrix}$. Dann ist $\varphi_2\left(\begin{pmatrix} a \\ b \\ c \end{pmatrix}\right) = A \begin{pmatrix} a \\ b \\ c \end{pmatrix}$. Um eine Basis des

Kerns zu bestimmen, wenden wir den Gauß an:

$$\begin{pmatrix} 1 & 2 & 2 \\ 2 & 3 & 1 \\ 1 & 0 & 1 \end{pmatrix} \begin{matrix} \\ |\,(-2) \\ \\ \end{matrix} \begin{matrix} \\ \longleftarrow + \\ \\ \end{matrix} \begin{matrix} \\ \\ |\,(-1) \\ \end{matrix} \begin{matrix} \\ \\ \longleftarrow + \end{matrix} \rightsquigarrow \begin{pmatrix} 1 & 2 & 2 \\ 0 & -1 & -3 \\ 0 & -2 & -1 \end{pmatrix} \begin{matrix} \\ |\,(-2) \\ \longleftarrow + \end{matrix} \rightsquigarrow \begin{pmatrix} 1 & 2 & 2 \\ 0 & -1 & -3 \\ 0 & 0 & 5 \end{pmatrix} \begin{matrix} \longleftarrow + \\ |\,2 \\ \end{matrix}$$

$$\rightsquigarrow \begin{pmatrix} 1 & 0 & -4 \\ 0 & 1 & 3 \\ 0 & 0 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 3 \\ 0 & 0 & 0 \end{pmatrix}.$$

Dann ist

$$\ker \varphi_2 = \ker A = \mathrm{LH}\left(\begin{pmatrix} 4 \\ 2 \\ 1 \end{pmatrix} \right).$$

Aufgabe 3 (*Körpererweiterungen als Vektorräume*) (*10 Punkte*)

a) Beweisen Sie, dass $\mathbb{F}_4$ genau einen Unterkorper $K \subset \mathbb{F}_4$ mit $K \neq \mathbb{F}_4$ besitzt und dass dieser isomorph zu $\mathbb{F}_2$ ist.

b) Gemäß Beispiel 4.1.3.(i) ist $\mathbb{F}_4$ ist somit ein $\mathbb{F}_2$-Vektorraum. Bestimmen Sie eine Basis dieses Vektorraums.

c) Bestimmen Sie einen $\mathbb{F}_2$-Vektorraumisomorphismus $(\mathbb{F}_2)^4 \to (\mathbb{F}_4)^2$.

Lösung zu Aufgabe 3

Die Verknüpfungstabellen von $\mathbb{F}_4$ sind

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

und

·	1	a	b
1	1	a	b
a	a	b	1
b	b	1	a

.

Hier sind a, b keine Variablen sondern bezeichnen konkrete Elemente von $\mathbb{F}_4$.

a) Die Elemente 0 und 1 müssen im Unterkörper K enthalten sein. Wäre nun noch $a \in K$, so müsste auch $1 + a = b \in K$ sein und es gälte $K = \mathbb{F}_4$ (analog gilt $b \in K \implies K = \mathbb{F}_4$). Daher muss $K = \{0, 1\}$ gelten und in der Tat ist das ein zweielementiger Unterkörper, also isomorph zu $\mathbb{F}_2$.

b) Bezeichne $B = \{1, b\}$. Wir zeigen, dass B eine Basis von L ist. Wir schreiben auf:

$$\begin{aligned} 0 \cdot_V 1 +_L 0 \cdot_V b &= 0 \\ 0 \cdot_V 1 +_L 1 \cdot_V b &= b \\ 1 \cdot_V 1 +_L 0 \cdot_V b &= 1 \\ 1 \cdot_V 1 +_L 1 \cdot_V b &= a. \end{aligned}$$

Wir sehen, dass die Linearkombination genau dann verschwindet, wenn die Koeffizienten verschwinden. Außerdem lässt sich jedes Element von L als Linearkombination von $1, b$ schreiben.

Bemerkung: Die Mengen $\{1, a\}$ und $\{a, b\}$ sind ebenfalls Basen.

c) Eine Basis von $(\mathbb{F}_2)^4$ ist durch

$$\left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\}$$

gegeben. Aus der Basis $\{1, b\}$ können wir die Basis

$$\left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} b \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ b \end{pmatrix}, \begin{pmatrix} b \\ b \end{pmatrix} \right\}$$

von $(\mathbb{F}_4)^2$ konstruieren.

Die Abbildung

$$(\mathbb{F}_2)^4 \to (\mathbb{F}_4)^2, \qquad \begin{pmatrix} v_1 \\ v_2 \\ v_3 \\ v_4 \end{pmatrix} \to \begin{pmatrix} v_1 + bv_2 \\ v_3 + bv_4 \end{pmatrix}$$

bildet die erste Basis bijektiv auf die zweite Basis ab und ist linear. Damit ist sie ein Vektorraumisomorphismus.

Aufgabe 4 (*Komplexe Vektorräume*) (*10 Punkte*)

Es sei $(V, +, \cdot)$ ein n-dimensionaler $\mathbb{C}$-Vektorraum mit $n \in \mathbb{N}$.
Beweisen Sie die folgenden Aussagen:

a) Durch Einschränkung der Skalarmultiplikation $\cdot\colon \mathbb{C} \times V \to V$ auf $\cdot|_{\mathbb{R}\times V}\colon \mathbb{R} \times V \to V$ erhält man daraus einen $\mathbb{R}$-Vektorraum $(V, +, \cdot|_{\mathbb{R}\times V})$.

b) Die Dimension von V als $\mathbb{R}$-Vektorraum ist $2n$.

c) Die Abbildung $J\colon V \to V, v \mapsto i \cdot v$ ist $\mathbb{R}$-linear und bijektiv. Bestimmen Sie die inverse Abbildung.

d) Es sei $\varphi\colon V \to V$ eine $\mathbb{R}$-lineare Abbildung. Zeigen Sie, dass φ genau dann $\mathbb{C}$-linear ist, wenn $\varphi \circ J = J \circ \varphi$ gilt.

Lösung zu Aufgabe 4

a) Man überzeugt sich, dass durch die Einschränkung der Skalarmultiplikation sich die Addition nicht ändert, die Distributivgesetze und die skalare Assoziativität gilt und das Element 1 weiterhin alle Vektoren erhält.

b) Sei $b_1, \ldots, b_n$ eine Basis von V als $\mathbb{C}$-Vektorraum. Dann beschreibt

$$B = \{b_1, ib_1, b_2, ib_2, \ldots, b_n, ib_n\}$$

eine Basis von V als $\mathbb{R}$-Vektorraum: Ist $v = a_1b_1 + \cdots + a_nb_n$ eine Linearkombination mit $a_i \in \mathbb{C}$ schreibe $a_i = x_i + iy_i$ mit $x_i, y_i \in \mathbb{R}$. Dann ist

$$v = (x_1 + iy_1)b_1 + \cdots + (x_n + iy_n)b_n = x_1b_1 + y_1ib_1 + \cdots + x_nb_n + y_nib_n$$

Damit haben wir gezeigt, dass B den $\mathbb{R}$-Vektorraum V erzeugt. Nun sei eine Linearkombination $\sum_i x_i b_i + \sum_i y_i i b_i = 0$ der Null gegeben. Dann ist

$$0 = \sum_i (x_i + iy_i) b_i$$

Da $b_1, \ldots, b_n$ eine Basis von V als $\mathbb{C}$-Vektorraum ist, gilt $x_i + iy_i = 0$. Also $x_i = 0 = y_i$ für alle i.

c) Seien $v, w \in V$. Dann ist

$$J(v+w) = i(v+w) = iv + iw = J(v) + J(w)$$

Ist weiterhin $\lambda \in \mathbb{R}$, dann ist

$$J(\lambda v) = i(\lambda v) = \lambda i v = \lambda J(v).$$

Also ist J eine lineare Abbildung. Man überlegt sich leicht, dass $v \mapsto -iv$ die zu J inverse Abbildung ist.

d) Wir zeigen zuerst die Hinrichtung. Dazu nehmen wir an, dass φ eine $\mathbb{C}$-lineare Abbildung ist. Dann ist

$$\varphi \circ J(v) = \varphi(iv) = i\varphi(v) = J \circ \varphi(v)$$

für alle $v \in V$. Also $\varphi \circ J = J \circ \varphi$.

Nun zeigen wir die Rückrichtung. Es gelte $\varphi \circ J = J \circ \varphi$. Seien $v \in V$ und $\lambda \in \mathbb{C}$. Wir schreiben $\lambda = a + ib$ mit $a, b \in \mathbb{R}$. Dann ist

$$\begin{aligned}
\varphi(\lambda v) &= \varphi((a+ib)v) \\
&= \varphi(av) + \varphi(ibv) \\
&= \varphi(av) + \varphi \circ J(bv) \\
&= \varphi(av) + J \circ \varphi(bv) \\
&= \varphi(av) + i\varphi(bv) \\
&= a\varphi(v) + ib\varphi(v) \\
&= \lambda \varphi(v).
\end{aligned}$$

Dass φ die Addition erhält, folgt schon daraus, dass φ eine $\mathbb{R}$-lineare Abbildung ist. Also haben wir gezeigt, dass φ eine $\mathbb{C}$-lineare Abbildung ist.

Aufgabe 5 (*Bonusaufgabe zu Weihnachten*) (*10 Punkte*)

Diese Aufgabe ist als Bonusaufgabe gedacht. Zur Bearbeitung haben Sie Zeit bis zum 18.01.21.

Wir betrachten die Matrix

$$A \coloneqq \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \end{pmatrix} \in \mathbb{F}_2^{12\times 12}$$

Bestimmen Sie die multiplikative Inverse A^{-1} von A. Was soll A^{-1}, als Pixelgrafik, darstellen?

Hinweis: Sie können die Inverse von A bestimmen, indem Sie den Gauß-Algorithmus auf die Blockmatrix $(A|\mathbb{1}_{12})$ anwenden. Die erweiterte Zeilenstufenform davon ist dann $(\mathbb{1}_{12}|A^{-1})$. Sie brauchen nicht zu begründen, warum das funktioniert.
Denken Sie daran, im Körper $\mathbb{F}_2$ und nicht in $\mathbb{R}$ zu rechnen.