Fachbereich Mathematik
Prof. Dr. J.H. Bruinier
Martin Fuchssteiner
Kay Schwieger

TECHNISCHE UNIVERSITÄT DARMSTADT

WS 07/08 22./23.11.07

Lineare Algebra I

6. Übung mit Lösungshinweisen

Gruppenübungen

Lemma 1. *Sei V ein Vektorraum über dem Körper $\mathbb{K}$. Seien $v_1, \dots, v_r \in V$ und $w_1, \dots, w_s \in V$ Vektoren mit*

(a) $s > r$

(b) Die Vektoren $w_1, \dots, w_s$ liegen in dem von den Vektoren $v_1, \dots, v_s$ aufgespannten, linearen Teilraum, d.h. es gibt Skalare $\alpha_{i,j} \in \mathbb{K}$ mit

$$w_i = \alpha_{1,i}v_1 + \alpha_{2,i}v_2 + \cdots + \alpha_{r,i}v_r \ .$$

Dann sind die Vektoren $w_1, \dots, w_s$ linear abhängig.

(G 1)

Sie haben Lemma 1 für den Spezialfall $V = \mathbb{R}^n$ und $\mathbb{K} = \mathbb{R}$ bereits in der Vorlesung gezeigt. Beweisen Sie Lemma 1 indem sie den Beweis aus der Vorlesung verallgemeinern.

LÖSUNG: Der Gauß-Algorithmus zum Lösen linearer Gleichungssysteme funktioniert analog auch für Matrizen über dem Körper $\mathbb{K}$. Das Gleichungssystem

$$\begin{aligned} \alpha_{1,1}\lambda_1 + \cdots + \alpha_{1,s}\lambda_s &= 0 \\ &\cdots \\ \alpha_{r,1}\lambda_1 + \cdots + \alpha_{r,s}\lambda_s &= 0 \end{aligned}$$

lässt sich damit in obere Dreiecksgestalt bzw. Diagonalgestalt bringen. Daraus folgt wie in der Vorlesung, dass dieses Gleichungssystem eine nicht-triviale Lösung $0 \neq (\tilde{\lambda}_1, \dots, \tilde{\lambda}_s) \in \mathbb{R}^s$ besitzt. Für diese Lösung gilt dann

$$\begin{aligned} \tilde{\lambda}_1 w_1 + \cdots + \tilde{\lambda}_s w_s &= \tilde{\lambda}_1 \Big(\sum_{j=1}^{r} \alpha_{1,j}\, v_j \Big) + \cdots + \tilde{\lambda}_s \Big(\sum_{j=1}^{r} \alpha_{s,j}\, v_j \Big) \\ &= \underbrace{\Big(\sum_{i=1}^{s} \alpha_{i,1}\, \tilde{\lambda}_i \Big)}_{=0} v_1 + \cdots + \underbrace{\Big(\sum_{i=1}^{s} \alpha_{i,r}\, \tilde{\lambda}_i \Big)}_{=0} v_r = 0 \ . \end{aligned}$$

Die Vektoren $w_1, \dots, w_s$ sind somit linear abhängig, weil nicht alle $\tilde{\lambda}_i$ Null sind.

Satz 1. *Sei $n \in \mathbb{N}$. Wir betrachten die Menge $\mathbb{Z}_n$ mit der Addition und Multiplikation (wie in der 5. Übung). $\mathbb{Z}_n$ ist genau dann ein Körper, wenn n eine Primzahl ist.*

(G 2)

Wir wollen Satz 1 in mehreren Schritten beweisen. Für die Elemente von $\mathbb{Z}_n$ schreiben wir wie in der 5. Übung $[x] = \{ y \in \mathbb{Z} \mid y \equiv x \pmod{n} \}$.

(a) In der 5. Übung haben Sie bereits einige Eigenschaften von $\mathbb{Z}_n$ gezeigt. Welche Körperaxiome haben Sie für $\mathbb{Z}_n$ bereits gezeigt, welche nicht?

(b) Sei $n \in \mathbb{N}$ keine Primzahl. Zeigen Sie, dass dann $\mathbb{Z}_n$ kein Körper ist.

Wir müssen damit nur noch zeigen, dass für einen Primzahl $p \in \mathbb{N}$ die Menge $\mathbb{Z}_p$ mit ihren Verknüpfungen tatsächlich einen Körper bildet. Sei also im Folgenden stets $p \in \mathbb{N}$ eine Primzahl. Mit Hilfe von Zerlegung in Primfaktoren kann man zeigen, dass für alle $x, y \in \mathbb{Z}$

$$p \mid x \cdot y \qquad \Longrightarrow \qquad p \mid x \quad \text{oder} \quad p \mid y$$

gilt. Zeigen Sie damit für alle $x, y \in \mathbb{Z}$:

(c) Gilt $[x \cdot y] = [0]$, so ist $[x] = [0]$ oder $[y] = [0]$.

(d) Gibt es ein $k \in \mathbb{N}$ mit $[x^k] = [0]$, so gilt $[x] = [0]$.

(e) Gibt es natürliche Zahlen $k_2 > k_1$ mit $[x^{k_1}] = [x^{k_2}]$, so ist $[x] = [0]$ oder $[x^{k_2 - k_1}] = [1]$.

Um den Beweis zu vervollständigen, zeigen Sie:

(f) Sei $x \in \mathbb{Z}$ mit $[x] \neq [0]$. Dann gibt es Exponenten $k_1 \neq k_2$ mit $[x^{k_1}] = [x^{k_2}]$.

Hinweis: Nutzen Sie, dass $\mathbb{Z}_p$ endlich ist.

(g) $\mathbb{Z}_p$ bildet einen Körper.

LÖSUNG: (a) Wir haben bereits gezeigt, dass $(\mathbb{Z}_n, +)$ eine abelsche Gruppe ist. Für die Multiplikation auf $\mathbb{Z}_n$ haben wir bereits gezeigt, dass sie assoziativ und kommutativ ist und mit der Addition das Distributivgesetz erfüllt.

Wir müssen noch zeigen, dass es in $\mathbb{Z}_n \setminus \{ [0] \}$ ein neutrales Element bzgl. der Multiplikation gibt und dass es für jedes Element $[x] \in \mathbb{Z}_n \setminus \{ [0] \}$ ein multiplikatives Inverses gibt.

(b) Wenn n keine Primzahl ist, gibt es ein Zahlen $x, y \in \mathbb{N}$ mit $1 < x, y < n$ und $n = x \cdot y$. Für die zugehörigen Kongruenzklassen ergibt sich damit

$$[n] = [x \cdot y] = [x] \cdot [y] \ .$$

Nach Konstruktion von $\mathbb{Z}_n$ gilt allerdings $[n] = [0]$. Wegen $1 < x, y < n$ sind x und y nicht durch n teilbar. In $\mathbb{Z}_n$ gilt damit $[x], [y] \neq [0]$. Nach Aufgabe G1.1 auf dem 5. Übungsblatt (Nullteilerfreiheit) kann $\mathbb{Z}_n$ somit kein Körper sein.

(c) Dies ist eine exakte Übersetzung der obigen Aussage, denn nach Konstruktion von $\mathbb{Z}_p$ gilt für alle $a \in \mathbb{Z}$

$$[a] = [0] \qquad \Longleftrightarrow \qquad a \equiv 0 \pmod{p} \qquad \Longleftrightarrow \qquad p \mid a \ .$$

(d) Wir zeigen die Behauptung mittels vollständiger Induktion über k. Der Induktionsanfang $k = 1$ ist trivial. Es gelte nun, dass aus $[x^k] = [0]$ bereits $[x] = 0$ folgt (Induktionsannahme). Für den Induktionsschritt sei $[x^{k+1}] = [0]$. Wegen $[0] = [x^{k+1}] = [x^k \cdot x] = [x^k] \cdot [x]$ folgt aus dem vorherigen Aufgabenteil, dass entweder $[x] = [0]$ oder $[x^k] = [0]$ gilt. Aufgrund der Induktionsannahme folgt in beiden Fällen $[x] = [0]$.

(e) Nach den Rechenregeln auf dem 5. Übungsblatt gilt

$$\begin{aligned}[0] &= [x^{k_2}] - [x^{k_1}] = [x^{k_1}] \cdot [x^{k_2-k_1}] - [x^{k_1}] \cdot [1] \\ &= [x^{k_1}] \cdot ([x^{k_2-k_1}] - [1]) = [x^{k_1}] \cdot [x^{k_2-k_1} - 1]\end{aligned}$$

Nach Aufgabenteil (c) folgt daraus $[x^{k_1}] = [0]$ oder $[x^{k_2-k_1} - 1] = [0]$. Im ersten Fall folgt aus Aufgabenteil (d) $[x] = 0$. Im zweiten Fall ergibt sich nach den Rechenregeln $[0] = [x^{k_2-k_1}] - [1]$ und somit $[x^{k_2-k_1}] = [1]$.

(f) Sei $x \in \mathbb{Z}$ mit $[x] \neq [0]$. Wir betrachten die Teilmenge $\{ [x^k] \mid k \in \mathbb{N} \}$ von $\mathbb{Z}_p$. In dieser Teilmenge können nicht alle Elemente verschieden sein, denn dann hätte diese Menge und damit auch $\mathbb{Z}_p$ unendlich viele Elemente. Es muss somit Zahlen $k_1, k_2 \in \mathbb{N}, k_1 \neq k_2$ geben mit $[x^{k_1}] = [x^{k_2}]$.

(g) In Aufgabenteil (a) haben wir gesehen, dass wir noch ein neutrales Element für die Multiplikation und zu jeden Element $[x] \neq [0]$ ein Inverses in $\mathbb{Z}_p$ finden müssen. Nach den Rechenregeln gilt für alle $x \in \mathbb{Z}$

$$[x] \cdot [1] = [x \cdot 1] = [x] = [1 \cdot x] = [1] \cdot [x] \ .$$

Das Element $[1] \in \mathbb{Z}_p$ ist damit ein neutrales Element für die Multiplikation.

Sei $[0] \neq [x] \in \mathbb{Z}_p$ mit $x \in \mathbb{Z}$. Nach Aufgabenteil (f) gibt es dann $k_1, k_2 \in \mathbb{N}$ mit $k_1 \neq k_2$ und $[x^{k_1}] = [x^{k_2}]$. Wir nehmen o.B.d.A. $k_2 > k_1$ an. Nach Aufgabenteil folgt daraus $[x] = [0]$ oder $[x^{k_2-k_1}] = [1]$. Nach Voraussetzung kann nicht $[x] = [0]$ gelten, es gilt somit $[x^{k_2-k_1}] = [1]$. Nach den Rechenregeln folgt

$$[1] = [x^{k_2-k_1}] = [x \cdot x^{k_2-k_1-1}] = [x] \cdot [x^{k_2-k_1-1}]$$

und analog $[x^{k_2-k_1-1}] \cdot [x] = [1]$. Das Element $[x^{k_2-k_1-1}]$ ist somit ein Inverses von $[x]$.

Hausübungen

(A 17) (10 Punkte)

Sei A eine $(m \times n)$-Matrix mit reellen Einträgen. Wir betrachten die zugehörige lineare Abbildung $\phi_A : \mathbb{R}^n \to \mathbb{R}^m$, $x \mapsto Ax$. Zeigen Sie, dass der Rang von A gleich der Dimension des Bildes von ϕ_A ist, d.h.

$$\operatorname{Rang} A = \dim(\operatorname{Bild} \phi_A) \ .$$

LÖSUNG: Wir bezeichnen für $1 \leq i \leq n$ mit $e_i \in \mathbb{R}^n$ den i-ten Einheitsvektor $e_i = (0, \dots, 0, 1, 0, \dots, 0)^T$ mit einer Eins an in der i-ten Koordinate. Weiter bezeichnen wir mit $a_1, \dots, a_n \in \mathbb{R}^m$ die Spalten von A, d.h. $A = (a_1 | \dots | a_n)$. Dann gilt für alle i

$$a_i = A \cdot e_i = \phi(e_i) \ .$$

Weil sich jeder Vektor $x \in \mathbb{R}^n$ als Linearkombination $x = \sum_{i=1}^n \lambda_i e_i$ der Einheitsvektoren schreiben lässt, kann jeder Bildvektor $\phi_A(x)$ auch als Linearkombination der Spalten von A dargestellt werden:

$$\phi_A(x) = \sum_{i=1}^n \lambda_i \phi_A(e_i) = \sum_{i=1}^n \lambda_i a_i \ .$$

$\operatorname{Bild} \phi_A = \{ \phi(x) \mid x \in \mathbb{R}^n \}$ wird also von den Spalten von A aufgespannt.

Wir wählen nun linear unabhängige Spalten $a_{i_1}, \dots, a_{i_r}$ mit $r = \operatorname{Rang} A$. Alle anderen Spalten hängen dann linear von $a_{i_1}, \dots, a_{i_r}$ ab und lassen sich deshalb als Linearkombination dieser Vektoren schreiben. Jeder Vektor in $\operatorname{Bild} \phi_A$ lässt sich deshalb als Linearkombination von $a_{i_1}, \dots, a_{i_r}$ darstellen. Die linear unabhängigen Vektoren $a_{i_1}, \dots, a_{i_r}$ erzeugen also $\operatorname{Bild} \phi_A$, d.h. sie bilden eine Basis von $\operatorname{Bild} \phi_A$:

$$\operatorname{Rang} A = r = \dim(\operatorname{Bild} \phi_A) \ .$$

(A 18) (10 Punkte)

Sei V ein Vektorraum über dem Körper $\mathbb{K}$. Zeigen Sie für alle $v \in V$ und $\lambda \in \mathbb{K}$:

(a) $0 \cdot v = 0$ und $\lambda \cdot 0 = 0$.

(b) $(-1) \cdot v = (-v)$.

(c) Gilt $\lambda \cdot v = 0$, so ist $\lambda = 0$ oder $v = 0$.

Sei $\mathbb{K}$ ein Körper. Zeigen Sie:

(d) Für je zwei Elemente $x, y \in \mathbb{K} \setminus \{0\}$ gibt es ein Element $z \in \mathbb{K}$ mit $x \cdot z = y$.

LÖSUNG: (a) Wegen der Distributivität gilt $0 \cdot v = (0+0) \cdot v = (0 \cdot v) + (0 \cdot v)$. Addiert man auf beiden Seiten der Gleichung das additive Inverse von $0 \cdot v$, ergibt sich die Behauptung.

(b) Wegen $1 \cdot v = v$ und der Distributivität ergibt sich mit den vorherigen Aufgabenteil

$$v + \big((-1) \cdot v\big) = (1 \cdot v) + \big((-1) \cdot v\big) = (1-1) \cdot v = 0 \cdot v = 0\,.$$

Durch Addition der Gleichung mit dem additiven Inversen von v ergibt sich dann die Behauptung.

(c) Sei $\lambda \cdot v = 0$. Ist $\lambda = 0$, ist die Behauptung bewiesen. Ist $\lambda \neq 0$, so ergibt sich mit dem ersten Aufgabenteil

$$0 = \lambda^{-1} \cdot 0 = \lambda^{-1}(\lambda \cdot v) = (\lambda^{-1}\,\lambda) \cdot v = 1 \cdot v = v\,.$$

(d) Für $z := x^{-1}y$ ergibt sich die Behauptung.

(A 19) (10 Punkte)

Wir wollen in dieser Aufgabe den Körper mit vier Elementen konstruieren. Hierzu betrachten wir das kartesische Produkt $\mathbb{K} := \mathbb{Z}_2 \times \mathbb{Z}_2$ und statten diese Menge mit der koordinatenweisen Addition aus:

$$+ : \mathbb{K} \times \mathbb{K} \to \mathbb{K}, \quad (a_1, a_2) + (b_1, b_2) := (a_1 + b_1, a_2 + b_2)$$

(a) Zeigen Sie, dass $(\mathbb{K}, +)$ eine abelsche Gruppe bildet.

(b) Zeige Sie, dass $\mathbb{K}$ mit der koordinatenweisen Multiplikation

$$\cdot : \mathbb{K} \times \mathbb{K} \to \mathbb{K}, \quad (a_1, a_2) \cdot (b_1, b_2) := (a_1 \cdot a_2, b_1 \cdot b_2)$$

keinen Körper bildet.

(c) Definieren Sie eine Multiplikation auf $\mathbb{K} = \mathbb{Z}_2 \times \mathbb{Z}_2$ mit $(1, 0)$ als neutralem Element, so dass $\mathbb{K}$ mit dieser Multiplikation und der koordinatenweisen Addition einen Körper bildet. (Auf den Nachweis des Distributivgesetztes können Sie verzichten.)

Hinweis: Die in Aufgabe A18 gezeigte Aussage könnte hilfreich sein.

LÖSUNG: (a) In Aufgabe T3 des 7. Tutoriums wird gezeigt, dass $G \times H$ mit der koordinatenweisen Multiplikation bzw. Addition wieder eine Gruppe bildet. Insbesondere bildet $\mathbb{K} = \mathbb{Z}_2 \times \mathbb{Z}_2$ eine Gruppe. Außerdem wird dort gezeigt, dass $G \times H$ genau dann abelsch ist, wenn G und H abelsch sind. Daraus folgt dann auch, dass $\mathbb{K} = \mathbb{Z}_2 \times \mathbb{Z}_2$ abelsch ist.

Alternativ kann man die Gesetze für die Elemente von $\mathbb{K}$ direkt nachrechnen. Das neutrale Element ist $(0, 0)$. Das inverse Element zu (a_1, a_2) ist $(-a_1, -a_2)$. Assoziativität und Kommutativität folgen direkt aus den entsprechenden Gesetzen für $\mathbb{Z}_2$.

(b) Es gilt $(1, 0) \cdot (0, 1) = (1 \cdot 0, 0 \cdot 1) = (0, 0)$. Dies widerspricht der Nullteilerfreiheit von Körpern.

(c) Wir versuchen die Verknüpfungstafel für die Multiplikation aufzustellen. Weil in jedem Körper $0 \cdot x = 0 = x \cdot 0$ und $1 \cdot x = 1 = x \cdot 1$ für jedes Element x gilt, muss die Verknüpfungstafel wie folgt aussehen:

$\cdot$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$
$(1,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,1)$	$(0,0)$	$(0,1)$		
$(1,1)$	$(0,0)$	$(1,1)$		

Wir müssen also nur noch vier Werte wählen. Weil die Multiplikation im Körper kommutativ ist, muss die Verknüpfungstafel spiegelsymmetrisch zur Diagonalen sein. Deshalb müssen nur noch drei Werte gesetzt werden: die beiden Diagonaleinträge und ein Eintrag neben der Diagonale.

Nach Aufgabe A18 muss in jeder Zeile und jeder Spalte bis auf die Zeile und Spalte für das Neutralelement $(0,0)$ jedes Element (genau) einmal vorkommen. Als Nebendiagonaleintrag $(0,1) \cdot (1,1) = (1,1) \cdot (0,1)$ können wir deshalb nicht $(1,1)$ setzen, denn in der entstehenden Verknüpfungstafel

$\cdot$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$
$(1,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,1)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(1,1)$	$(0,0)$	$(1,1)$	$(1,1)$	?

würde in der untersten Zeile bereits $(1,1)$ doppelt auftreten. Es verbleibt deshalb nur eine Möglichkeit:

$\cdot$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$
$(1,0)$	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
$(0,1)$	$(0,0)$	$(0,1)$	$(1,1)$	$(1,0)$
$(1,1)$	$(0,0)$	$(1,1)$	$(1,0)$	$(0,1)$

Wir haben bereits gezeigt, dass $(\mathbb{K}, +)$ eine abelsche Gruppe bildet. Weil auf den Beweis der Distributivität verzichtet werden soll, können wir uns ganz auf die Multiplikation konzentrieren. Die Verknüpfungstafel ist bereits so konstruiert, dass die Verknüpfung ein neutrales Element $(1,0)$ besitzt und kommutativ (spiegelsymmetrisch zur Diagonalen) ist. Somit bleibt nur die Assoziativität der Multiplikation zu zeigen. Weil wir die Verknüpfung gerade so konstruiert haben, dass $(1,0)$ das neutrale Element der Multiplikation ist und $x \cdot (0,0) = (0,0) = (0,0) \cdot x$ für alle Elemente $x \in \mathbb{K}$ gilt, genügt es die Assoziativität für die Elemente $(0,1)$ und $(1,1)$ zu zeigen. Hierzu rechnen wir direkt nach:

$$\begin{aligned}
(0,1) \cdot \big((0,1) \cdot (0,1)\big) &= (1,0) = \big((0,1) \cdot (0,1)\big) \cdot (0,1) \\
(0,1) \cdot \big((0,1) \cdot (1,1)\big) &= (0,1) = \big((0,1) \cdot (0,1)\big) \cdot (1,1) \\
(0,1) \cdot \big((1,1) \cdot (1,1)\big) &= (1,1) = \big((0,1) \cdot (1,1)\big) \cdot (1,1) \\
(1,1) \cdot \big((1,1) \cdot (1,1)\big) &= (1,0) = \big((1,1) \cdot (1,1)\big) \cdot (1,1)
\end{aligned}$$

Entweder man rechnet nun auch die restlichen Produkte von $(0,1)$ und $(1,1)$ aus oder man überlegt sich, dass (und wie) die Assoziativität für alle anderen Produkte aus der Kommutativität der Verknüpfung folgt.