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

TECHNISCHE UNIVERSITÄT DARMSTADT

WS 2007/2008

Lineare Algebra I

5. Übung mit Lösungshinweisen

Gruppenübungen

MINITEST

(T 1) Gegeben seien die folgenden Matrizen:

$$A = \begin{pmatrix} 1 & 2 \end{pmatrix} B = \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \quad C = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \quad D = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}.$$

Welche der folgenden Ausdrücke sind dann definiert?

☐ AB ☐ BA ☐ $A+B$ ☐ CD ☐ DC ☐ C^2 ☐ D^2

(T 2)

Welche der folgenden Ausdrücke sind für beliebige $n \times n$–Matrizen A und B und die Einheitsmatrix E_n richtig?

☐ $(A+B)^2 = A^2 + 2AB + B^2$ ☐ $(A+B)(A-B) = A^2 - B^2$

☐ $(A+E_n)(A-E_n) = A^2 - E_n$

(G 1) Körper

Beweisen Sie, daß die folgenden Aussagen für einen Körper $\mathbb{K}$ richtig sind:

1. $\forall a \in \mathbb{K} : a \cdot 0 = 0 = 0 \cdot a$
2. $\forall a, b \in \mathbb{K} : a \cdot b = 0 \Rightarrow a = 0 \vee b = 0$ (Nullteilerfreiheit)
3. $\forall a, b \in \mathbb{K} : a \cdot (-b) = -(ab) = (-a)b$
4. $\forall a, b \in \mathbb{K} : (-a) \cdot (-b) = ab$

LÖSUNG:

1. Es gilt $a \cdot 0 = a \cdot (0 + 0) = (a \cdot 0) + (a \cdot 0)$ für alle $a \in \mathbb{K}$. Zieht man nun von beiden Seiten der Gleichung $a \cdot 0$ ab, so erhlt man $0 = a \cdot 0$. Da die Multiplikation kommutativ ist, gilt somit auch $0 \cdot a = 0$.
2. Es gelte $a \cdot b = 0$ für zwei Elemente $a, b \in \mathbb{K}$. Ist b nicht die Null, so kann man beide Seiten der Gleichung von Rechts mit b^{-1} multiplizieren. Durch Rechtsmultiplikation mit dem Inversen b^{-1} zu b erhält man $a = a(b \cdot b^{-1}) = 0 \cdot b^{-1} = 0$, d.h. $a = 0$.
3. Es gilt $ab + a(-b) = a(b - b) = a \cdot 0 = 0$ für alle $a, b \in \mathbb{K}$. Somit ist $a(-b)$ das Inverse von ab bezüglich der Addition, d.h. $a(-b) = -(ab)$.

4. Nach Teilaufgabe 3 gilt $(-a)(-b) = -(-ab)$ für alle $a, b \in \mathbb{K}$. Somit folgt $(-ab) + (-a)(-b) = (-ab) - (-ab) = 0$ für alle $a, b \in \mathbb{K}$, d.h. $(-a)(-b)$ ist das Inverse von $-ab$ bezüglich der Addition, d.h. $(-a)a(-b) = (ab)$.

(G 2) Äquivalenzrelationen (Wiederholung)

Es sei $n \geq 2$ eine natürliche Zahl. Zwei Zahlen $a, b \in \mathbb{Z}$ heißen *kongruent modulo* n, geschrieben $a \equiv b \pmod{n}$, falls die ganze Zahl $a - b$ durch n teilbar ist.

(a) Beweisen Sie, daß die Kongruenz $\equiv \pmod{n}$ modulo n eine Äquivalenzrelation ist, d.h. daß folgende Bedingungen erfüllt sind:

1. $\forall a \in \mathbb{Z} : a \equiv a \pmod{n}$ (Reflexivität)
2. $\forall a, b \in \mathbb{Z} : (a \equiv b \pmod{n}) \Rightarrow (b \equiv a \pmod{n})$ (Symmetrie)
3. $\forall a, b, c \in \mathbb{Z} : (a \equiv b \pmod{n}) \wedge (b \equiv c \pmod{n}) \Rightarrow a \equiv c \pmod{n}$ (Transitivität)

(b) Zeigen Sie, daß die Kongruenz $\equiv \pmod{n}$ modulo n sogar eine Kongruenzrelation ist, d.h. daß zusätzlich die Bedingungen

1. $\forall a, b, c, d \in \mathbb{Z} : (a \equiv b \pmod{n}) \wedge (c \equiv d \pmod{n}) \Rightarrow (a + c \equiv b + d \pmod{n})$
2. $\forall a, b, c, d \in \mathbb{Z} : (a \equiv b \pmod{n}) \wedge (c \equiv d \pmod{n}) \Rightarrow (a \cdot c \equiv b \cdot d \pmod{n})$

erfüllt sind.

LÖSUNG:

(a)

1. Da $a - a$ immer durch n teilbar ist, gilt $a \equiv a \pmod{n}$.
2. Gilt $a \equiv b \pmod{n} \Leftrightarrow n \mid (a - b)$, so gibt es eine ganzen Zahl $c \in \mathbb{Z}$, so daß $n \cdot c = (a - b)$ erfüllt ist. Somit gilt auch $n \cdot (-c) = (b - a)$, d.h. $b \equiv a \pmod{n}$.
3. Aus $a \equiv b \pmod{n}$ und $b \equiv c \pmod{n}$ folgt die Existenz ganzer Zahlen $d, e \in \mathbb{Z}$, so daß die Gleichungen $n \cdot d = (a - b)$ und $n \cdot e = (c - a)$ erfüllt sind. durch Addition dieser Gleichungen erhält man $n \cdot (d + e) = (c - b) + (a - b) = (c - a)$, es folt $a \equiv c \pmod{n}$.

(b) Es seien $a, b, c, d \in \mathbb{Z}$ ganze Zahlen, für welche $a \equiv b \pmod{n}$ und $c \equiv d \pmod{n}$ gelte. Es gibt somit ganze Zahlen e und f, so daß die Gleichungen $n \cdot e = (a - b)$ und $n \cdot f = (d - c)$ erfüllt sind.

1. Durch Addition der Gleichungen $n \cdot e = (a - b)$ und $n \cdot f = (d - c)$ erhält man $n \cdot (e + f) = (b - a) + (d - c) = (b + d) - (a + c)$. Somit gilt $a + c \equiv b + d \pmod{n}$.
2. Durch Unformen der Gleichungen $n \cdot e = (a - b)$ und $n \cdot f = (d - c)$ erhält man $b = a + n \cdot e$ und $d = c + n \cdot f$. Multipliziert man nun diese Gleichungen, so ergibt sich $bd = ac + n \cdot (af + ce) + n^2 = ac + n \cdot (af + ce + n)$. Es folgt $n \cdot (af + ce + n) = bd - ac$. Somit gilt $a \cdot c \equiv b \cdot d \pmod{n}$.

(G 3) Restklassenringe

Es sei $\mathbb{Z}$ der Ring der ganzen Zahlen und $n \geq 2$ eine natürliche Zahl. Die *Kongruenzklasse* $[a]$ modulo n einer ganzen Zahl a ist die Menge $\{z \in \mathbb{Z} \mid z \equiv a \pmod{n}\}$ aller zu a kongruenten ganzen Zahlen. Die Menge aller dieser Kongruenzklassen wird mit $\mathbb{Z}_n$ bezeichnet.

(a) Beweisen Sie, daß sich die Addition und die Multiplikation von $\mathbb{Z}$ auf $\mathbb{Z}_n$ übertragen, d.h. daß die Operationen $[a] + [b] := [a + b]$ und $[a] \cdot [c] = [a \cdot c]$ wohldefiniert sind.

(b) Zeigen Sie, daß $\mathbb{Z}_n$ mit obiger Addition eine kommutative Gruppe ist. Welches ist hier das neutrale Element?

(c) Beweisen Sie, daß die Multiplikation in $\mathbb{Z}_n$ assoziativ und kommutativ ist sowie daß das Distributivgesetz gilt.

(d) Zeigen Sie daß $\mathbb{Z}_2$ mit obiger Addition und Multiplikation ein Körper ist. Geben Sie die Gruppentafel fur die Gruppen $(\mathbb{Z}_n, +, [0])$ und $(\mathbb{Z}_n \setminus \{[0]\}, \cdot, [1])$ an.

LÖSUNG:

(a) Es ist zu Beweisen, daß für Ganze Zahlen $a, b, c, d \in \mathbb{Z}$ aus $[a] = [c]$ und $[b] = [d]$ auch $[a + b] = [c + d]$ folgt. Gilt $[a] = [c]$ und $[b] = [d]$, so folgt $c \in [a]$ und $d \in [b]$, d.h. $a \equiv c \pmod n$ und $b \equiv d \pmod n$. Aus Aufgabe G2 b) ergibt sich nun $a + b \equiv c + d \pmod n$, d.h. $[a + b] = [c + d]$.
Der Beweis der Wohldefiniertheit der Multiplikation verläuft analog: Gilt $[a] = [c]$ und $[b] = [d]$, so folgt $c \in [a]$ und $d \in [b]$, d.h. $a \equiv c \pmod n$ und $b \equiv d \pmod n$. Aus Aufgabe G1 b) ergibt sich nun $a \cdot b \equiv c \cdot d \pmod n$, d.h. $[a \cdot b] = [c \cdot d]$.

(b) Aus den Gruppeneigenschaften von $(\mathbb{Z}, +, 0)$ folgt

1. $([a] + [b]) + [c] = [a + b] + [c] = [(a + b) + c] = [a + (b + c)] = [a] + ([b + c]) = [a] + ([b] + [c])$ (Assoziativität)
2. $[a] + [0] = [a] = [0] + [a]$ (Neutrales Element)
3. $[a] + [-a] = [0] = [-a] + [a]$ (Existenz eines Inversen Elementes)
4. $[a] + [b] = [a + b] = [b + a] = [b] + [a]$ (Kommutativität)

für alle $[a], [b], [c] \in \mathbb{Z}_n$. Somit ist $(\mathbb{Z}_n, +, [0])$ eine kommutative Gruppe. Die Gruppentafel ist folgende:

$$\begin{array}{c|cc} + & [0] & [1] \\ \hline [0] & [0] & [1] \\ & [1] & [0] \end{array}$$

(c) Dies folgt analog zu teilaufgabe b): Es gilt

1. $([a] \cdot [b]) \cdot [c] = [a \cdot b] \cdot [c] = [(a \cdot b) \cdot c] = [a \cdot (b \cdot c)] = [a] \cdot ([b \cdot c]) = [a] \cdot ([b] \cdot [c])$ (Assoziativität)
2. $[a] \cdot [b] = [a \cdot b] = [b \cdot a] = [b] \cdot [a]$ (Kommutativität)
3. $[a] \cdot ([b] + [c]) = [a] \cdot [b + c] = [a \cdot (b + c)] = [ab + ac] = [a] \cdot [b] + [a] \cdot [c]$ (Distributivität)

für alle $[a], [b], [c] \in \mathbb{Z}_n$.

(d) Hier ist zu Zeigen:

1. Die Menge $\mathbb{Z}_2 \setminus \{[0]\}$ mit Multiplikation ist eine kommutative Gruppe.
2. Es gilt das Assoziativ- und dass Distributivgesetz.

Die Menge $\mathbb{Z}_2$ besteht nur aus der Kongruenzklasse $[1]$. Die Multiplikation ist durch $[1] \cdot [1] = [1]$ gegeben. Sie ist assoziativ kommutative und es gibt eine Inverses element zu $[1]$ (nämlich $[1]$ selber). Somit ist $(\mathbb{Z}_2 \setminus \{[0]\}, 0, [1])$ eine kommutative Gruppe. Die Gruppentafel ist folgende:

$$\begin{array}{c|c} \cdot & [1] \\ \hline [1] & [1] \end{array}$$

Die Assoziativität und die Distributivität wurde schon in Aufgabenteil b) bewiesen.

(G 4)

Es sei $\mathbb{R}[x] = \{a_n x^n + \ldots + a_1 x + a_0 \mid n \in \mathbb{N}, a_n, \ldots, a_0 \in \mathbb{R}\}$ die Menge aller reellen Polynome. Bekanntlich können zwei Polynome addiert und multipliziert und mit einer reellen Zahl skalar multipliziert werden. Für die reellen Polynome $p = \sum_{i=0}^n p_i x^i$ und $q = \sum_{i=0}^n q_i x^i$ $(n \in \mathbb{N})$ und die reelle Zahl λ gilt:

$$
\begin{aligned}
p + q &= \sum_{i=0}^{n} (p_i + q_i) x^i, && \text{Addition} \\
p \cdot q &= \sum_{i,j=0}^{n} p_i q_j x^{i+j}, && \text{Multiplikation} \\
\lambda \cdot p &= \sum_{i=0}^{n} \lambda p_i x^i && \text{Skalarmultiplikation.}
\end{aligned}
$$

Bemerkung: Da die Koeffizienten p_i und q_i $(i \in \{1, \ldots, n\})$ auch gleich Null sein dürfen, beinhalten die obige Definition auch die Addition und Multiplikation von Polynomen unterschiedlichen Grades.

(a) Zeige, daß $(\mathbb{R}[x], +, \cdot)$ ein $\mathbb{R}$-Vektorraum ist. (b) Ist $(\mathbb{R}[x], +, \cdot)$ auch ein Körper?

LÖSUNG:

(a) Da für $p = \sum_{i=0}^n p_i x^i$, $q = \sum_{i=0}^n q_i x^i$ und $r = \sum_{i=0}^n r_i x^i$

$$(p + q) + r = \sum_{i=0}^{n} ((p_i + q_i) + r_i) x^i = \sum_{i=0}^{n} (p_i + (q_i + r_i)) x^i = p + (q + r)$$

gilt, ist $(\mathbb{R}[x], +)$ eine Halbgruppe.

Das Nullpolynom ist das neutrale Element der Addition, da für alle $p \in \mathbb{R}[x]$ die Gleichung $0 + p = p$ gilt. Außerdem ist $-p$ das Inverse von p. Folglich ist $(\mathbb{R}[x], +)$ eine Gruppe.

Da

$$p + q = \sum_{i=0}^{n} (p_i + q_i) x^i = \sum_{i=0}^{n} (q_i + p_i) x^i = q + p$$

gilt, ist $(\mathbb{R}[x], +)$ eine kommutative Gruppe.

Für $p, q \in \mathbb{R}[x]$ und $\lambda, \mu \in \mathbb{R}$ gilt

$$
\begin{aligned}
(\lambda + \mu) \cdot p &= \sum_{i=0}^{n} (\lambda + \mu) p_i x^i = \sum_{i=0}^{n} \lambda p_i x^i + \sum_{i=0}^{n} \mu p_i x^i = \lambda \cdot p + \mu \cdot p, \\
\lambda \cdot (p + q) &= \sum_{i=0}^{n} \lambda (p_i + q_i) x^i = \sum_{i=0}^{n} \lambda p_i x^i + \sum_{i=0}^{n} \lambda q_i x^i = \lambda \cdot p + \lambda \cdot q, \\
\lambda \cdot (\mu \cdot p) &= \sum_{i=0}^{n} \lambda (\mu p_i) x^i = \sum_{i=0}^{n} (\lambda \mu) p_i x^i = (\lambda \mu) \cdot p, \\
1 \cdot p &= \sum_{i=0}^{n} 1 \cdot p_i x^i = \sum_{i=0}^{n} p_i x^i = p.
\end{aligned}
$$

Insgesamt folgt daraus, daß $(\mathbb{R}[x], +, \cdot)$ ein $\mathbb{R}$-Vektorraum ist.

(b) Der Ring $(\mathbb{R}[x], +, \cdot)$ besitzt offensichtlich ein Einselement, nämlich das konstante Polynom 1. Allerdings existieren im Allgemeinen keine multiplikativen Inversen. Zum Beispiel gilt für $p \in \mathbb{R}[x]$ und $x \in \mathbb{R}[x]$

$$p \cdot x = \sum_{i=0}^{n} p_i x^{i+1} \neq 1,$$

weshalb x kein multiplikatives Inverses besitzt. Folglich ist $(\mathbb{R}[x], +, \cdot)$ kein Körper.

Hausübungen

(A 14) (10 Punkte)

(a) Beweisen Sie, daß $\mathbb{Z}_3$ mit der Addition und der Multipliaktion aus Aufgabe G 3 ein Körper ist und geben Sie die Gruppentafeln für $(\mathbb{Z}_3, +, [0])$ und $(\mathbb{Z}_3 \setminus \{[0]\}, \cdot, [1])$ an.

(b) Zeigen Sie, daß $\mathbb{Z}_4$ in obigem Sinne kein Körper ist.

LÖSUNG:

(a) Es ist schon bekannt, daß $(\mathbb{Z}_3, +, [0])$ eine kommutative Gruppe ist. Die Gruppentafel ist

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
	[1]	[2]	[0]
	[2]	[0]	[1]

Daher bleibt nur noch zu beweisen, daß auch $(\mathbb{Z}_3 \backslash \{[0\}, \cdot, [1])$ eine kommutative Gruppe ist. Die Verknüpfungstafel ist

·	[0]	[1]	[2]
[0]	[0]	[0]	[0]
	[0]	[1]	[2]
	[0]	[2]	[1]

(b) Es gilt $[2] + [2] = [4] = [0]$. Das Element $[2]$ kann somit kein Inverses $[2]^{-1}$ haben, da sonst $[0] = [0] \cdot [2]^{-1} = ([2] + [2])[2]^{-1} = [2][2]^{-1} + [2][2]^{-1} = [1] + [1] = [2]$ gelten müsste, was nicht sein kann.

(A 15) (10 Punkte)

(a) In jeder Zeile und jeder Spalte der folgenden Verknüpfungstafel kommt jedes Element genau einmal vor. Trotzdem handelt es sich nicht um eine Gruppentafel. Warum nicht?

	e	a	b	c	d
e	e	a	b	c	d
a	a	e	c	d	b
b	b	d	e	a	c
c	c	b	d	e	a
d	d	c	a	b	e

(b) Es seien s und t ganze Zahlen. Man betrachte auf $\mathbb{Z}$ die Verknüpfung $\odot$ mit $a \odot b := sa + tb$ (für alle $a, b \in \mathbb{Z}$). Für welche s, t ist diese Verknüpfung assoziativ bzw. kommutativ?

LÖSUNG:

(a) Die Verknüpfung ist nicht assoziativ, beispielsweise gilt $(ab)d = cd = a$, aber $a(bd) = ac = d$.

(b) Es gilt
$$(a \odot b) \odot c = (sa + tb) \odot c = s(sa + tb) + tc = s^2 a + stb + tc$$
und analog
$$a \odot (b \odot c) = a \odot (sb + tc) = sa + t(sb + tc) = sa + tsb + t^2 c,$$
also ist die Verknüpfung genau dann assoziativ, falls $(s^2 - s)a = (t^2 - t)c$ für alle $a, c \in \mathbb{Z}$. Diese Gleichung ist für $s, t \in \{0, 1\}$ erfüllt. Entsprechend erhält man aus
$$a \odot b = sa + tb = sb + ta = b \odot a$$
die Gleichung $a(s - t) = b(s - t)$, welche genau für $s = t$ erfüllt ist.

(A 16) (10 Punkte)

Sei $A := \mathbb{R}\backslash\{1\}$. Auf $A \times A$ definieren wir eine Abbildung $\odot$ durch $a \odot b := a + b - ab$. Man zeige, dass $\odot$ eine Verknüpfung und $(A, \odot)$ eine kommutative Gruppe ist.

LÖSUNG:

Zunächst ist die Wohldefiniertheit der Verknüpfung zu zeigen. Mit anderen Worten: gibt es Zahlen $a, b \in A$, so dass $a \odot b \notin A$? Angenommen, es gibt solche Zahlen $a, b \in A$ mit $a + b - ab = 1$. Dann folgt $b(1 - a) = 1 - a$. Da $a \in A$ ist $1 - a$ nicht Null und wir können kürzen. Es folgt $b = 1$, was einen Widerspruch zur Annahme darstellt. Die Verknüpfung ist mithin wohldefiniert. Nun zu den Gruppeneigenschaften. Seien dazu $a, b, c \in A$ beliebig gewählt. Dann gilt:
$$\begin{aligned} a \odot (b \odot c) = a \odot (b + c - bc) = a + b + c - bc - a(b + c - bc) = \\ a + b + c - ab - (a + b - ab)c = (a + b - ab) \odot c = (a \odot b) \odot c \end{aligned}$$
sowie
$$a \odot b = a + b - ab = b + a - ba = b \odot a.$$
Um das neutrale Element $e \in A$ zu bestimmen, machen wir den Ansatz $a \odot e = a + e - ae = a$, woraus $(1 - a)e = 0$ und damit $e = 0$ folgt, da $1 - a \neq 0$. Aus der bereits gezeigten Kommutativität folgt, dass e auch linksneutral ist, $e \odot a = a$. Den gleichen Ansatz machen wir für das Inverse b zu einem gewählten $a \in A$. Es muss gelten $a \odot b = a + b - ab = 0$, folglich ist $b = \frac{a}{a-1}$ rechtsinvers zu a. Ebenso folgt aus der Kommutativität, dass dieses Element auch linksinvers ist.