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

TECHNISCHE UNIVERSITÄT DARMSTADT

WS 2007/2008 9.10.2007

Lineare Algebra I

1. Tutorium mit Lösungshinweisen

(T 1)

Für zwei ganze Zahlen a, c schreiben wir $a|c$, falls a die Zahl c teilt. Beweisen oder widerlegen Sie die folgenden Aussagen. Machen Sie sich dabei bewußt, was genau zu tun ist, um eine Aussage zu beweisen bzw. zu widerlegen.

(a) Gilt $a|b$ und $b|c$, so folgt $a|d$.

(b) Gilt $a|b$ und $b|a$, so folgt $a = b$ oder $a = -b$.

(c) Gilt $a|b$ und $a|c$, so gilt auch $a|(b+c)$ und $a|(b-c)$.

(d) Gilt $a|c$ und $b|c$, so folgt $(a+b)|c$.

(e) Gilt $a|b$, so gilt für jede Zahl c auch $a|b \cdot c$.

(f) Gilt $a|c$ und $b|c$, so gilt auch $(a \cdot b)|c$.

LÖSUNG:

(a) Es gelte $a \mid b$ und $b \mid c$. Dann gibt es $k_a, k_b \in \mathbb{Z}$ mit $b = k_a \cdot a$ und $c = k_b \cdot b$. Durch Einsetzen ergibt sich $c = (k_b \cdot k_a) \cdot a$, also teilt a die Zahl c.

(b) Es gelte $a \mid b$ und $b \mid a$. Dann gibt es $k_a, k_b \in \mathbb{Z}$ mit $a = k_b \cdot b$ und $b = k_a \cdot a$. Durch Einsetzen ergibt sich $a = k_b \cdot k_a \cdot a$. Mit der Kürzungsregel folgt $k_b \cdot k_a = 1$. Somit sind k_a und k_b beide 1 oder beide -1. Es ergibt sich $a = k_a b = \pm b$.

(c) Es gelte $a \mid b$ und $b \mid c$. Dann gibt es $k_b, k_c \in \mathbb{Z}$ mit $b = k_b \cdot a$ und $c = k_c \cdot a$. Durch Einsetzen ergibt sich $b \pm c = k_b a + k_c a = (k_b + k_c) \cdot a$, also $a \mid (b \pm c)$.

(d) Gegenbeispiel: Es gilt $1 \mid 1$ und $1 \mid 1$, aber nicht $(1+1) \mid 1$.

(e) Es gelte $a \mid b$. Außerdem sei $c \in \mathbb{Z}$ eine ganze Zahl. Wegen $a \mid b$ gibt es eine Zahl $k \in \mathbb{Z}$ mit $b = k \cdot a$. Durch Multiplikation von c erhalten wir $c b = c k a$, also $a \mid (c \cdot b)$.

(f) Gegenbeispiel: Es gilt $2 \mid 2$ und $2 \mid 2$, aber nicht $(2 \cdot 2) \mid 2$.

(T 2)

Schreiben Sie die Aussagen aus Aufgabe T1 mit Hilfe des Quantors $\forall$ (Für alle), des Zeichens $\wedge$ für "und", des Zeichens $\vee$ für "oder" und mit Hilfe des Implikationspfeils $\Rightarrow$. Die Aussage aus Aufgabe T1 a) läßt sich z.B. durch "$\forall a, b, c \in \mathbb{Z} : a \mid b \wedge b \mid c \Rightarrow a \mid c$" kurz schreiben.

LÖSUNG:

(a) $\forall a, b, c \in \mathbb{Z} : (a \mid b \wedge b \mid c) \;\Rightarrow\; a \mid c$

(b) $\forall a, b \in \mathbb{Z} : (a \mid b \wedge b \mid a) \;\Rightarrow\; (a = b \vee a = -b)$.

(c) $\forall a, b \in \mathbb{Z} : (a \mid b \wedge a \mid c) \;\Rightarrow\; (a \mid (b+c) \wedge a \mid (b-c))$.

(d) $\forall a, bc \in \mathbb{Z} : (a \mid c \wedge b \mid c) \Rightarrow (a+b) \mid c$.

(e) $\forall a, b \in \mathbb{Z} : a \mid b \Rightarrow (\forall c \in \mathbb{Z} : a \mid b \cdot c)$.

(f) $\forall a, b \in \mathbb{Z} : (a \mid c \wedge b \mid c) \Rightarrow (a \cdot b) \mid c$.

(T 3) Kongruenzklassen

Es sei $n \geq 2$ eine natürliche Zahl. Wir nennen zwei Zahlen a, b *kongruent modulo n*, falls die ganze Zahl $a - b$ durch n teilbar ist. Wir schreiben in diesem Fall $a \equiv b \pmod{n}$.

(a) Für welche Zahlen a gilt $a \equiv 0 \pmod 2$, für welche gilt $a \equiv 1 \pmod 2$?

(b) Zeige, daß $a \equiv 0 \pmod n$ genau dann gilt, wenn $n|a$ gilt.

Hinweis: Die Satzkonstruktion „genau dann ..., wenn“ beinhaltet *zwei* Implikationen.

(c) Zeige, daß $a \equiv b \pmod n$ genau dann gilt, wenn a und b denselben Rest bei Division durch n haben. Formuliere hierzu vor dem Beweis genau, was du unter dem Rest bei Division durch n verstehst.

(d) Zeige: Gilt $a \equiv b \pmod n$ und $c \equiv d \pmod n$, so gilt auch

$$a \pm c \equiv b \pm d \pmod n \qquad \text{und} \qquad a \cdot c \equiv b \cdot d \pmod n\,.$$

LÖSUNG:

(a) $a \equiv 0 \pmod 2$ gilt genau für alle geraden Zahlen, und $a \equiv 1 \pmod 2$ gilt genau für alle ungerade Zahlen.

(b) Nach Definition gilt $a \equiv 0 \pmod n$ genau dann, wenn die Differenz $a - 0 = a$ durch n teilbar ist.

(c) Definition: Sei a eine ganze Zahl. Der *Rest von a bei Division durch n* ist diejenige (eindeutig bestimmte) Zahl $r_a \in \{0, 1, \dots, n-1\}$, für welche es eine ganze Zahl k gibt mit

$$a = k \cdot n + r_a\,.$$

Eine Implikation: Seien a, b ganze Zahlen mit $a \equiv b \pmod n$. Wir bezeichnen mit r_a bzw. r_b den Rest von a bzw. b bei Division durch n. Nach Definition gibt es ganze Zahlen k_a, k_b mit

$$a = k_a \cdot n + r_a\,, \qquad\qquad b = k_b \cdot n + r_b\,.$$

Wegen $a \equiv b \pmod n$ ist die Differenz $a - b = (k_a - k_b) \cdot n + (r_a - r_b)$ durch n teilbar. Weil das Produkt $(k_a - k_b) \cdot n$ trivial durch n teilbar ist, folgt mit Aufgabe T1 (c), daß auch die Differenz $r_a - r_b = (a - b) - (k_a - k_b) \cdot n$ durch n teilbar ist. Wegen $0 \leq r_a, r_b \leq n - 1$, gilt für die Differenz $-n + 1 \leq r_a - r_b \leq n - 1$. Die einzige durch n teilbare Zahl in diesem Intervall ist 0, also $r_a - r_b = 0$.

Die andere Implikation: Seien a, b ganze Zahlen mit demselben Rest $r \in \{0, \dots, n-1\}$ bei Division durch n. Dann gibt es ganze Zahlen k_a, k_b mit

$$a = k_a \cdot n + r\,, \qquad\qquad b = k_b \cdot n + r\,.$$

Die Differenz $a - b = (k_a - k_b) \cdot n$ somit durch n teilbar.

(T 4)

(a) Zeige, daß es für jede natürliche Zahl a genau eine Zahl $k \in \{0,1,2,3\}$ mit $a \equiv k \pmod 4$ gibt!

Hinweis: Die Satzkonstruktion „genau eine“ ist gleichbedeutend mit „eine und *nur* eine“.

(b) Wieviele Primzahlen p gibt es mit $p \equiv 0 \pmod 4$, wieviele mit $p \equiv 2 \pmod 4$?

(c) Gibt es unendlich viele Primzahlen p mit $p \equiv 3 \pmod 4$? Die folgenden Teilaufgaben können dir vielleicht bei deiner Entscheidung helfen:

1. In der Vorlesung wurde gezeigt, daß es unendlich viele Primzahlen gibt. Diskutiere in deiner Gruppe die wesentlichen Schritte des Beweises!
2. Zeige, daß für alle natürlichen Zahlen $a_1, \ldots, a_n$ gilt:

$$\prod_{i=1}^{n}(4a_i+1) \equiv 1 \pmod 4 ,$$
$$\prod_{i=1}^{n}(4a_i+3) \equiv (-1)^n \pmod 4 .$$

(d) (Für Interessierte) Gibt es unendlich viele Primzahlen p mit $p \equiv 1 \pmod 4$?

LÖSUNG:

(a) Sei a eine natürliche Zahl. Sei $k \in \{0,1,2,3\}$ ihr Rest bei Division durch n. Dann gilt $a \equiv k \pmod 4$ mit Aufgabe T3 (c).

(b) Es gibt keine Primzahl mit $p \equiv 0 \pmod{}$ und genau eine Primzahl mit $p \equiv 2 \pmod 4$, nmlich 2.

(c)
1. ...
2. Für jede natürliche Zahl a gilt $4a+1 \equiv 1 \pmod 4$ und $4a+3 \equiv (-1) \pmod 4$ (siehe Aufgabe T3 (d)). Mit Aufgabe T3 (d) ergibt sich deshalb für die Produkte:

$$(4a_1+1)(4a_2+1)\ldots(4a_n+1) \equiv \underbrace{1 \cdot 1 \cdot \ldots \cdot 1}_{n \text{ Stck}} \equiv 1 \pmod 4 ,$$
$$(4a_1+3)(4a_2+3)\ldots(4a_n+3) \equiv \underbrace{(-1)\cdot(-1)\cdot\ldots\cdot(-1)}_{n \text{ Stck}} = (-1)^n \pmod 4 .$$

Es gibt unendlich viele Primzahlen p mit $p \equiv 3 \pmod 4$. Wir führen den Beweis völlig analog zu dem Beweis aus der Vorlesung für die Existenz unendlich vieler Primzahlen:
Wir nehmen an, daß es nur endlich viele solche Primzahlen $p_1, \ldots, p_n$ gibt. Weil all diese Primzahlen den Rest 3 bei Division durch 4 haben, gibt es natürliche Zahlen $a_1, \ldots, a_n$ mit $p_i = 4a_i + 3$ für jeden Index i. Wir betrachten die Zahl

$$\hat{p} := p_1 \cdot p_2 \cdot \ldots \cdot p_n + 3 - (-1)^n = \prod_{i=1}^{n}(4a_i+3) + 3 - (-1)^n .$$

I. $\hat{p} \equiv 3 \pmod 4$:
Nach Aufgabenteil T4 (c) 2 ist das Produkt $p_1 \ldots p_n = \prod_{i=1}^{n}(4a_i+3)$ kongruent zu $(-1)^n$ modulo 4. Für $\hat{p}$ gilt also

$$\hat{p} \equiv (-1)^n + 3 - (-1)^n = 3 \pmod 4 .$$

II. $\hat{p}$ ist durch kein p_i teilbar.
Bei Division durch eine der Primzahlen p_i ergibt sich für $\hat{p}$ der Rest $3-(-1)^n$, denn es gilt
$$\hat{p} = p_1 p_2 \dots p_n + 3 - (-1)^n \equiv 0 + 3 - (-1)^n \pmod{p_i} .$$
Wäre $\hat{p}$ durch eine der Primzahlen p_i teilbar, so müsste sich der Rest 0 ergeben.

III. $\hat{p}$ ist nicht durch 2 teilbar.
Wäre $\hat{p}$ durch 2 teilbar (also $\hat{p}$ gerade), so müsste sich bei der Division durch 4 der Rest 0 oder Rest 2 ergeben. Es gilt jedoch $\hat{p} \equiv 3 \pmod 4$.

Zerlegen wir $\hat{p}$ in Primfaktoren $\hat{p} = q_1 \cdot \ldots \cdot q_m$, so treten dabei nur Primzahlen q_i mit $q_i \equiv 1 \pmod 4$ auf. Für jede solche Primzahl q_i gibt es eine natürliche Zahl b_i mit $q_i = 4b_i + 1$. Damit ergibt sich $\hat{p}$ als Produkt
$$\hat{p} = \prod_{i=1}^{m} (4b_i + 1) .$$
Nach Aufgabenteil T4 (c) 2 besitzt ein solches Produkt den Rest 1 bei Division durch 4. Dies steht jedoch im Widerspruch zu $\hat{p} \equiv 3 \pmod 4$.

(d) Ja, weil … – finde es doch selbst heraus!