Universität Konstanz
Fachbereich Mathematik und Statistik
Prof. Dr. Markus Schweighofer
Aaron Kunert / Sven Wagner

Wintersemester 2009/2010
Lösungsblatt 5
02.12.2009

Lineare Algebra I

Lösung 5.1:

Voraussetzung: Sei A ein kommutativer Ring.

(a) Behauptung: Sind $a, b, b' \in A$ mit $ab = 1 = ab'$, so gilt $b = b'$.
Beweis: Da 1 das neutrale Element der Multiplikation ist, und die Multiplikation assoziativ und kommutativ ist, gilt $b = 1 \cdot b = ab'b = b'ab = b' \cdot 1 = b'$.

(b) Behauptung: Für $a \in A$ ist $(a) := \{ab \mid b \in A\}$ ein Ideal von A.
Beweis: Das wurde in der Vorlesung gezeigt.

(c) Behauptung: $\mathbb{Z}/(7)$ ist ein Körper.
Beweis: 7 ist eine Primzahl. Also ist nach der Vorlesung $\mathbb{Z}/(7) = \mathbb{F}_7$ ein Körper. Alternativ sieht man das folgendermaßen: Sei $\equiv := \equiv_7$. Dann ist $\mathbb{Z}/(7)$ ein kommutativer Ring mit $\overline{1}$ als neutralem Element der Multiplikation, da (7) ein Ideal von $\mathbb{Z}$ ist und 1 das neutrale Element der Multiplikation in $\mathbb{Z}$ ist. Es gilt $\overline{0} \neq \overline{1}$, da 1 in $\mathbb{Z}$ nicht durch 7 teilbar ist. Nun gilt $\overline{2} \cdot \overline{4} = \overline{8} = \overline{1}$, $\overline{3} \cdot \overline{5} = \overline{15} = \overline{1}$ und $\overline{6} \cdot \overline{6} = \overline{36} = \overline{1}$. Damit haben wir alles gezeigt.

(d) Behauptung: In $\mathbb{Z}/(12)$ gibt es zwei Elemente $a, b \neq 0$ mit $ab = 0$.
Beweis: Es ist $12 = 2 \cdot 6$, aber $2, 6 \notin (12)$. Also gilt in $\mathbb{Z}/(12)$, dass die Klassen von 2 und 6 nicht 0 sind, sehr wohl aber deren Produkt.

(e) Behauptung: $\mathbb{Z}/(777)$ ist kein Körper.
Beweis: Es ist $777 = 7 \cdot 111$, somit ist 777 keine Primzahl. Also ist nach dem Satz aus der Vorlesung $\mathbb{Z}/(777)$ kein Körper. Alternativ sieht man das auch so: Wie in Aufgabenteil (d) finden wir in $\mathbb{Z}/(777)$ zwei Elemente a und b mit $a, b \neq 0$ und $ab = 0$ (z.B. die Klassen von 7 und 111). Dies kann aber in einem Körper nicht vorkommen: Wäre $\mathbb{Z}/(777)$ ein Körper, so gäbe es, da $a \neq 0$ ist, ein $a' \in \mathbb{Z}/(777)$ mit $a'a = 1$. Dann wäre aber $b = 1 \cdot b = a'ab = a' \cdot 0 = 0$, ein Widerspruch zu $b \neq 0$.

Lösung 5.2:

Voraussetzung: Sei A ein kommutativer Ring und $\equiv$ eine Kongruenzrelation auf A.

(a) Behauptung: Für alle $n \in \mathbb{N}_0$ und alle $a, b \in A$ gilt

$$a \equiv b \Rightarrow a^n \equiv b^n.$$

Beweis: Induktionsanfang: Wir beginnen mit $n = 0$. Seien $a, b \in A$. Dann ist $a^0 = 1 = b^0$. Hier stimmt also die Aussage sogar unabhängig von der Kongruenzrelation.
Induktionsannahme: Wir nehmen an, dass die Aussage für ein festes $n \in \mathbb{N}_0$ gilt.
Induktionsschritt: Wir zeigen, dass die Aussage dann auch für $n+1$ gilt. Seien $a, b \in A$ mit $a \equiv b$. Nach Induktionsannahme wissen wir, dass dann auch $a^n \equiv b^n$ gilt. Da aber $\equiv$ eine Kongruenzrelation auf A ist, folgt daraus schon $a \cdot a^n \equiv b \cdot b^n$, also $a^{n+1} \equiv b^{n+1}$.

(b) Behauptung: Für alle Polynome $p \in A[X]$ und alle $a, b \in A$ gilt

$$a \equiv b \Rightarrow p(a) \equiv p(b).$$

Beweis: Sei $p = \sum_{k=0}^{n} a_k X^k \in A[X]$ (mit $n \in \mathbb{N}_0$), und seien $a, b \in A$ mit $a \equiv b$. Nach Aufgabenteil (a) gilt $a^k \equiv b^k$ für $k = 0, \ldots, n$. Da $\equiv$ eine Kongruenzrelation auf A ist, gilt außerdem noch $a_k a^k \equiv a_k b^k$ für $k = 0, \ldots, n$. Aus dem gleichen Grund gilt dann schließlich auch, dass die endlichen Summen $\sum_{k=0}^{n} a_k a^k$ und $\sum_{k=0}^{n} a_k b^k$ zueinander kongruent sind.

Lösung 5.3:

1. Wir dividieren mit Rest: $47 = 3 \cdot 13 + 8$. Es ergibt sich also $47 \bmod 13 = 8$.
2. Wir dividieren analog zu oben mit Rest: $379 = 18 \cdot 21 + 1$. Also ist $379 \bmod 21 = 1$.
3. Hier benutzen wir einen Trick. Wir schreiben

$$\begin{aligned} 1267987658 = {} & 1 \cdot 1000000000 \\ & + 2 \cdot 100000000 \\ & + 6 \cdot 10000000 \\ & + 7 \cdot 1000000 \\ & + 9 \cdot 100000 \\ & + 8 \cdot 10000 \\ & + 7 \cdot 1000 \\ & + 6 \cdot 100 \\ & + 5 \cdot 10 \\ & + 8 \cdot 1 \end{aligned}$$

Dazu bemerken wir, dass $10^k \bmod 9 = 1$ gilt. Dies ergibt sich daraus, dass die Zahl $10^k - 1 = \underbrace{99\ldots9}_{k-\text{mal}} = 9 \cdot \underbrace{11\ldots1}_{k-\text{mal}}$ ist. Dadurch vereinfacht sich die Rechnung wie folgt

$$12367987658 \equiv_{\langle 9 \rangle} 1 + 2 + 6 + 7 + 9 + 8 + 7 + 6 + 5 + 8 \equiv_{\langle 9 \rangle} 59.$$

Wir erhalten $12367987658 \bmod 9 = 5$.

4. Wir haben

$$\begin{aligned} 17^5 &\equiv_{\langle 10 \rangle} 7^5 \\ &\equiv_{\langle 10 \rangle} 49 \cdot 49 \cdot 7 \\ &\equiv_{\langle 10 \rangle} 9 \cdot 9 \cdot 7 = 81 \cdot 7 \\ &\equiv_{\langle 10 \rangle} 1 \cdot 7 \\ &\equiv_{\langle 10 \rangle} 7 \end{aligned}$$

Also ist $17^5 \bmod 10 = 7$

5. Wie in der Aufgabe zuvor gezeigt, ist $398 \equiv_{\langle 21 \rangle} 1$ und daher ist $398^{101} \bmod 21 = 1^{101} = 1$.

6. Es ist $823 \bmod 21 = 4$. Also genügt es $4^{2009} \bmod 21$ zu berechnen. Es ist

$$\begin{aligned} 4^1 &\equiv_{\langle 21\rangle} 4 \\ 4^2 &\equiv_{\langle 21\rangle} 16 \\ 4^3 &\equiv_{\langle 21\rangle} 1 \\ 4^4 &\equiv_{\langle 21\rangle} 4^3 \cdot 4 \equiv_{\langle 21\rangle} 4 \\ 4^5 &\equiv_{\langle 21\rangle} 4^3 \cdot 16 \equiv_{\langle 21\rangle} 16 \\ &\vdots \qquad\qquad \vdots \end{aligned}$$

   Wir sehen nun also, wie sich die Potenzen von 4 im Ring $\mathbb{Z}/\langle 21\rangle$ verhalten. Es ist

$$823^{2009} \equiv_{\langle 21\rangle} 4^{2009} \equiv_{\langle 21\rangle} 4^{1000+1000+9} \equiv_{\langle 21\rangle} 4^{3\cdot 333+1} \cdot 4^{3\cdot 333+1} \cdot 4^{3\cdot 3} \equiv_{\langle 21\rangle} 4 \cdot 4 \cdot 1 = 16.$$

   Also ist hier $823^{209} \bmod 21 = 16$.

7. Dies ist eine Kombination der letzten Methoden. Wir reduzieren zuerst die Basis modulo 9: $8903783438 \equiv_{\langle 9\rangle} 8$. Analog zur letzten Aufgabe betrachten wir die Potenzen

$$\begin{aligned} 8^1 &\equiv_{\langle 9\rangle} 8 \\ 8^2 &\equiv_{\langle 9\rangle} 1 \end{aligned}$$

   Daher ist

$$8903783438^{20567} \equiv_{\langle 9\rangle} 8^{20567} \equiv_{\langle 9\rangle} 8^{2\cdot 10282+1} \equiv_{\langle 9\rangle} 1^{10282} + 8 \equiv_{\langle 9\rangle} 8.$$

   So ist schließlich $8903783438^{20567} \bmod 9 = 8$.

Lösung 5.4:

Es ist $\mathcal{P}(\{1,2,3\}) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$. Sei $M \in A = (\mathcal{P}(\{1,2,3\}), \triangle, \cap)$ beliebig. Für alle $n \in \mathbb{N}$ gilt $M^n = \bigcap_{i=1}^{n} M = M$. Außerdem gilt $-M = M$, da $M \triangle M = \varnothing$.
Es ist $0 = \varnothing$ und $1 = \{1,2,3\}$ in A. Somit ist

$$p(M) = (M+M+\{1,3\}M+\{1,2,3\})(M+\{1,2\}) = \big((\{1,3\}\cap M)\triangle\{1,2,3\}\big)\cap(M\triangle\{1,2\}).$$

Nun betrachten wir alle Mengen $M \in A$ einzeln.

$$\begin{aligned} \varnothing\text{:}\ & \big((\{1,3\}\cap\varnothing)\triangle\{1,2,3\}\big)\cap(\varnothing\triangle\{1,2\}) = \{1,2,3\}\cap\{1,2\} = \{1,2\} \\ \{1\}\text{:}\ & \big((\{1,3\}\cap\{1\})\triangle\{1,2,3\}\big)\cap(\{1\}\triangle\{1,2\}) = \{2,3\}\cap\{2\} = \{2\} \\ \{2\}\text{:}\ & \big((\{1,3\}\cap\{2\})\triangle\{1,2,3\}\big)\cap(\{2\}\triangle\{1,2\}) = \{1,2,3\}\cap\{1\} = \{1\} \\ \{3\}\text{:}\ & \big((\{1,3\}\cap\{3\})\triangle\{1,2,3\}\big)\cap(\{3\}\triangle\{1,2\}) = \{1,2\}\cap\{1,2,3\} = \{1,2\} \\ \{1,2\}\text{:}\ & \big((\{1,3\}\cap\{1,2\})\triangle\{1,2,3\}\big)\cap(\{1,2\}\triangle\{1,2\}) = \{2,3\}\cap\varnothing = \varnothing \\ \{1,3\}\text{:}\ & \big((\{1,3\}\cap\{1,3\})\triangle\{1,2,3\}\big)\cap(\{1,3\}\triangle\{1,2\}) = \{2\}\cap\{2,3\} = \{2\} \\ \{2,3\}\text{:}\ & \big((\{1,3\}\cap\{2,3\})\triangle\{1,2,3\}\big)\cap(\{2,3\}\triangle\{1,2\}) = \{1,2\}\cap\{1,3\} = \{1\} \\ \{1,2,3\}\text{:}\ & \big((\{1,3\}\cap\{1,2,3\})\triangle\{1,2,3\}\big)\cap(\{1,2,3\}\triangle\{1,2\}) = \{2\}\cap\{3\} = \varnothing \end{aligned}$$

Lösung 5.5:

Voraussetzung: Sei A ein kommutativer Ring. Wir betrachten die abelsche Gruppe $(A^{\mathbb{N}_0}, +)$ aus § 2.1 der Vorlesung bzw. aus Aufgabe 3.3. Die **Faltung** $f * g$ von f und g aus $A^{\mathbb{N}_0}$ sei definiert durch $(f * g)(k) = \sum_{i=0}^{k} f(i)g(k-i)$ für $k \in \mathbb{N}_0$.

1. Behauptung: $(A^{\mathbb{N}_0}, +, *)$ ist ein kommutativer Ring.
   Beweis: Seien $f, g, h \in A^{\mathbb{N}_0}$.
   Kommutativität: Sei $k \in \mathbb{N}_0$. Dann ist

$$(f * g)(k) = \sum_{i=0}^{k} f(i)g(k-i) = \sum_{i=0}^{k} f(k-i)g(i) = \sum_{i=0}^{k} g(i)f(k-i) = (g * f)(k).$$

   Assoziativität: Sei $k \in \mathbb{N}_0$. Es gilt

$$\big((f * g) * h\big)(k) = \sum_{i=0}^{k} (f * g)(i)h(k-i) = \sum_{i=0}^{k} \sum_{j=0}^{i} f(j)g(i-j)h(k-i).$$

   Man beachte, dass stets $j+(i-j)+(k-i) = k$ gilt, und für $l, m, n \in \mathbb{N}_0$ mit $l+m+n = k$ gibt es genau eine Wahl von $i \in \{0, \ldots, k\}$ und $j \in \{0, \ldots, i\}$, bei der $l = j$, $m = i - j$ und $n = k - i$ ist. Salopp könnte man also statt $\sum_{i=0}^{k} \sum_{j=0}^{i} f(j)g(i-j)h(k-i))$ auch $\sum_{l+m+n=k} f(l)g(m)h(n)$ schreiben. Aber diese Summe ist wegen $m + n = k - l$ und $n = k - l - m$ mit der Summe $\sum_{l=0}^{k} \sum_{m=0}^{k-l} f(l)g(m)h(k-l-m))$ identisch. Es gilt aber

$$\sum_{l=0}^{k} \sum_{m=0}^{k-l} f(l)g(m)h(k-l-m) = \sum_{l=0}^{k} f(l)(g * h)(k-l) = \big(f * (g * h)\big)(k).$$

   Neutrales Element: $1 := (1, 0, 0, \ldots)$ ist neutral bezüglich $*$: Sei $k \in \mathbb{N}_0$. Nach Definition ist $(f * 1)(k) = \sum_{i=0}^{k} f(i)1(k-i)$. Es ist für $i < k$ stets $1(k-i) = 0$ und für $k = i$ ist $1(k-i) = 1(0) = 1$. Somit ist $(f * 1)(k) = f(k)$.
   Distributivität: Sei $k \in \mathbb{N}_0$. Es gilt

$$\begin{aligned} f * (g + h) &= \sum_{i=0}^{k} f(i)(g+h)(k-i) = \sum_{i=0}^{k} f(i)(g(k-i) + h(k-i)) \\ &= \sum_{i=0}^{k} f(i)g(k-i) + \sum_{i=0}^{k} f(i)h(k-i) = (f * g)(k) + (f * h)(k) \\ &= \big((f * g) + (f * h)\big)(k). \end{aligned}$$

2. Behauptung: Es gilt $(1, -1, 0, 0, 0, \ldots) * f = 1$ für $f = (1, 1, 1, \ldots)$.
   Beweis: Sei $g := (1, -1, 0, 0, 0, \ldots)$. Dann ist

$$(g * f)(0) = g(0)f(0) = 1 \cdot 1 = 1$$

   und für $k \in \mathbb{N}$

$$(g * f)(k) = \sum_{i=0}^{k} g(i)f(k-i) = 1 \cdot f(k) + (-1) \cdot f(k-1) = 1 \cdot 1 + (-1) \cdot 1 = 0.$$

3. Behauptung $(1,-1,-1,0,0,0,\dots) * f = 1$, wenn f die Folge der Fibonacci-Zahlen ist, allerdings beginnend mit der ersten 1 und nicht, wie üblich, der 0: $1,1,2,3,5,8,13,21,\dots$.
Genauer $f(0) := 1, f(1) := 1$ und für $k > 1$ sei $f(k) := f(k-1) + f(k-2)$.
Beweis: Sei $g := (1,-1,-1,0,0,\dots)$. Dann ist

$$(g * f)(0) = g(0)f(0) = 1 \cdot 1 = 1$$

und für $k \in \mathbb{N}$

$$\begin{aligned}(g * f)(k) &= \sum_{i=0}^{k} g(i)f(k-i) = 1 \cdot f(k) + (-1) \cdot f(k-1) + (-1)f(k-2) \\ &= f(k) - (f(k-1) + f(k-2)) = 0.\end{aligned}$$