Lineare Algebra II
Lösungsvorschläge zum Tutoriumsblatt 2

Moritz Fleischmann

Zur Vorlesung von Prof. Dr. Fabien Morel, Dr. Andrei Lavrenov, Katharina Novikov und Oliver Hendrichs im Sommersemester 25

Disclaimer: Das sind keine offiziellen Lösungen, sondern nur eine getexte Version der Lösungen zu ausgewählten Aufgaben (Dank geht hierbei an Andrei Lavrenov für seine Lösungsskizzen), die ich in meinem Tutorium bespreche. Fehler, Fragen oder Anmerkungen gerne an m.fleischmann@mnet-online.de . Gebt die Lösungen gern weiter, wenn ihr wollt.

Wie üblich, wen das Vorgeplänkel nicht interessiert, der kann die Lösungen in den grau hinterlegten Boxen finden. Es gilt grundsätzlich, dass $\mathbb{K} \subseteq \mathbb{C}$.

Aufgabe 1

Mit $\mathbb{P}$ bezeichnen wir die Menge der Primzahlen.

1. Sei $p \in \mathbb{P}, n \in \mathbb{Z}$ mit $p \nmid n$. Zeige, dass die natürliche Abbildung
$$\begin{aligned} \varphi : \mathbb{Z}/pn\mathbb{Z} &\to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ a + pn\mathbb{Z} &\mapsto (a + p\mathbb{Z}, a + n\mathbb{Z}) \end{aligned}$$
ein Isomorphismus ist.
2. Seien $p_1, \dots, p_m \in \mathbb{P}_+$ paarweise verschieden. Zeige
$$\mathbb{Z}/p_1 \cdot \ldots \cdot p_m\mathbb{Z} \simeq \mathbb{Z}/p_1\mathbb{Z} \times \ldots \times \mathbb{Z}/p_m\mathbb{Z}$$

Lösung:

1. Um zu zeigen, dass φ ein Isomorphismus ist, zeigen wir zuerst, dass φ wohldefiniert ist. Dann zeigen wir, dass φ ein Homomorphismus ist und danach Bijektivität.
   (a) *Wohldefiniertheit:* Wir müssen zeigen, dass eine Äquivalenzklasse in $\mathbb{Z}/pn\mathbb{Z}$ nur auf eine einzige Äquivalenzklasse in $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ abgebildet wird. Da unsere Abbildung bezüglich Repräsentanten definiert ist, müssen wir zeigen, dass zwei Repräsentanten einer Äquivalenzklasse in $\mathbb{Z}/pn\mathbb{Z}$ auf Repräsentanten einer einzigen Äquivalenzklasse in $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ abgebildet wird.
   Seien $a, b \in [a] \in \mathbb{Z}/pn\mathbb{Z}$, dann gilt $\exists k \in \mathbb{Z} : a = b + kpn$, dann gilt aber auch $a = b + (kn)p$ und $a = b + (kp)n$, also sind a, b auch in $\mathbb{Z}/p\mathbb{Z}$ und $\mathbb{Z}/n\mathbb{Z}$ in der gleichen Äquivalenzklasse. Daraus folgt direkt $\varphi(a + pn\mathbb{Z}) = \varphi(b + pn\mathbb{Z})$ und die Abbildung ist wohldefiniert.
   (b) *Homomorphismus:* Wir müssen zeigen, dass φ mit der Addition und Multiplikation verträglich ist. Seien also $a, b \in \mathbb{Z}/pn\mathbb{Z}$, dann gilt:
$$\begin{aligned} \varphi(a + b + pn\mathbb{Z}) &= (a + b + p\mathbb{Z}, a + b + n\mathbb{Z}) \\ &= (a + p\mathbb{Z}, a + n\mathbb{Z}) + (b + p\mathbb{Z}, b + n\mathbb{Z}) \\ &= \varphi(a + pn\mathbb{Z}) + \varphi(b + pn\mathbb{Z}) \end{aligned}$$
   hierbei verwenden wir, dass die Projektion $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ mit der Addition kommutiert, also $[a] + [b] = [a + b]$ gilt. Analog funktioniert das auch mit der Multiplikation, deswegen

gilt:

$$\begin{aligned}\varphi(a \cdot b + pn\mathbb{Z}) &= (a \cdot b + p\mathbb{Z}, a \cdot b + n\mathbb{Z}) \\ &= (a + p\mathbb{Z}, a + n\mathbb{Z}) \cdot (b + p\mathbb{Z}, b + n\mathbb{Z}) \\ &= \varphi(a + pn\mathbb{Z}) \cdot \varphi(b + pn\mathbb{Z})\end{aligned}$$

Da beide Eigenschaften gelten ist φ ein Homomorphismus.

(c) *Bijektivität:* Wir verwenden folgende Aussage: Ist $f : A \to B$ eine Abbildung und gelte $|A| = |B| < \infty$, dann folgt:

$$f \text{ injektiv } \Leftrightarrow f \text{ surjektiv } \Leftrightarrow f \text{ bijektiv}$$

Zeigen wir also, dass $\mathbb{Z}/pn\mathbb{Z}$ und $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ die gleiche (endliche) Anzahl an Elementen haben, reicht es bereits aus Injektivität *oder* Surjektivität zu zeigen um Bijektivität zu erhalten.
Wir können die Elemente von $\mathbb{Z}/k\mathbb{Z}$ einfach auflisten, denn

$$\mathbb{Z}/k\mathbb{Z} = \{[0], [1], \ldots, [k-1]\} \Rightarrow |\mathbb{Z}/k\mathbb{Z}| = k$$

Das kartesische Produkt zweier Mengen hat als Mächtigkeit das Produkt der Mächtigkeiten, es gilt also

$$|\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}| = |\mathbb{Z}/p\mathbb{Z}| \cdot |\mathbb{Z}/n\mathbb{Z}| = p \cdot n$$

und offensichtlich hat $\mathbb{Z}/pn\mathbb{Z}$ auch pn Elemente, das heißt es reicht aus die Injektivität zu zeigen.
Wir zeigen die Injektivät über den Kern, denn ein Homomorphismus ist genau dann injektiv, wenn sein Kern nur die 0 enthält. Sei $a + pn\mathbb{Z} \in \ker(\varphi)$, dann gilt

$$\varphi(a + pn\mathbb{Z}) = (a + p\mathbb{Z}, a + n\mathbb{Z}) = (0 + p\mathbb{Z}, 0 + n\mathbb{Z})$$

das heißt a ist Vielfaches von p und Vielfaches von n, oder anders gesagt $p \mid a$ und $n \mid a$. Es gibt also $y \in \mathbb{Z}$, sodass $a = yn$. Insbesonder gilt dann $p \mid yn$. Da p eine Primzahl ist, teilt p damit entweder n oder y. Da wir am Anfang angenommen haben, dass $p \nmid n$, folgt also $y = xp$ für ein geeignetes $x \in \mathbb{Z}$. Insgesamt gilt also $a = xpn$, das heißt $np \mid a$ und $a \equiv 0 \mod pn$, das heißt unser Kern ist trivial und die Abbildung bijektiv.

Aus diesen drei Eigenschaften folgt, dass φ ein Isomorphismus ist.

2. Diese Aufgabe ist mit Induktion zu lösen. Wir induzieren über die Anzahl der Primzahlen:

   (a) *Induktionsanfang:* Für zwei verschiedene Primzahlen p_1, p_2 gilt $p_1 \nmid p_2$, also folgt das direkt aus Teilaufgabe 1.

   (b) *Induktionsvoraussetzung:* Für jeweils m verschiedene Primzahlen gilt genannte Aussage.

   (c) *Induktionsschritt:* $m \to m + 1$. Es seien nun $p_1, \ldots, p_{m+1}$ paarweise verschiedene Primzahlen. Es gilt

$$p_{m+1} \nmid p_1 \cdot \ldots \cdot p_m$$

also können wir die erste Teilaufgabe anwenden und erhalten

$$\mathbb{Z}/p_1 \cdot \ldots \cdot p_{m+1}\mathbb{Z} \simeq \mathbb{Z}/p_1 \cdot \ldots \cdot p_m\mathbb{Z} \times \mathbb{Z}/p_{m+1}\mathbb{Z}$$

und mit der Induktionsvoraussetzung gilt

$$\mathbb{Z}/p_1 \cdot \ldots \cdot p_m\mathbb{Z} \simeq \mathbb{Z}/p_1\mathbb{Z} \times \ldots \times \mathbb{Z}/p_m\mathbb{Z}$$

also insgesamt

$$\mathbb{Z}/p_1 \cdot \ldots \cdot p_{m+1}\mathbb{Z} \simeq \mathbb{Z}/p_1\mathbb{Z} \times \ldots \times \mathbb{Z}/p_{m+1}\mathbb{Z}$$

was wir zeigen wollten.

Mit vollständiger Induktion folgt, dass diese Aussage für alle m gilt.

Aufgabe 2

1. Es sei $x \in \mathbb{Z}$, sodass $x \equiv 3 \mod 5$ und $x \equiv 2 \mod 7$. Nenne alle möglichen x.
2. Finde alle $x \in \mathbb{Z}$, sodass $x \equiv 3 \mod 5, x \equiv 2 \mod 7$ und $x \equiv 2 \mod 3$.

Lösung:
Wir verwenden hier den kleinen Satz von Fermat:

Seien $a \in \mathbb{Z}$ und $p \in \mathbb{P}$, dann gilt:

$$a^p \equiv a \mod p$$

Gilt außerdem $p \nmid a$, dann gilt auch:

$$a^{p-1} \equiv 1 \mod p \Rightarrow a^{p-2} \equiv a^{-1} \mod p$$

1. Wir stellen unser x in der Form $x = 5a + 7b$ dar. Das hat den Vorteil, dass wir beide Gleichungen getrennt betrachten können. Denn es gilt

$$x = 5a + 7b \equiv 7b \mod 5$$

und analog auch $x \equiv 5a \mod 7$. Wir betrachten also folgende Gleichungen:

$$5a \equiv 2 \mod 7$$
$$7b \equiv 3 \mod 5$$

Die Lösung dieser Gleichung bestimmen wir wie folgt: Kennen wir ein a', sodass $5a' \equiv 1 \mod 7$ gilt, dann löst $a = 2a'$ unsere Gleichung (und analog $b = 3b'$). Wir bestimmen also zuerst $a' \equiv 5^{-1} \mod 7$ und $b' \equiv 7^{-1} \mod 5$. Es gilt mit dem kleinen Satz von Fermat:

$$5^{7-2} \equiv 5^{-1} \mod 7 \Rightarrow a' \equiv 5^5 \mod 7 \equiv 3 \mod 7$$
$$7^{5-2} \equiv 7^{-1} \mod 5 \Rightarrow b' \equiv 7^3 \mod 5 \equiv 3 \mod 5$$

Daraus erhalten wir also $a = 6 \equiv 6 \mod 7$ und $b = 9 \equiv 4 \mod 5$. Damit haben wir schon eine Lösung gefunden. Jede weiter Lösung finden wir, indem wir andere Repräsentanten der

Äquivalenzklassen einsetzen. Es gilt also

$$x = 5 \cdot (6 + 7k) + 7 \cdot (4 + 5l) \equiv 23 \mod 35$$

2. Es gilt $3 \nmid 35$, die Aufgabe könnte also ähnlich zur ersten Aufgabe gelöst werden (35 ist zwar keine Primzahl, es gilt aber trotzdem $3 \nmid 35$). Wir sehen hier aber direkt, dass

   $$23 \equiv 2 \mod 3$$

   also haben wir bereits eine Lösung gefunden. Sei x' nun eine weitere Lösung. Da x' ebenfalls in der gleichen Äquivalenzklasse bezüglich $3, 5, 7$ liegen muss, muss die Differenz $x' - 23$ ein Vielfaches von $3, 5$ und 7 sein. Deshalb gilt

   $$x' \equiv 23 \mod 105$$

Aufgabe 3
Es sei $\mathbb{K}$ ein Körper, $P(X) \in \mathbb{K}[X]$ mit $\deg(P) = n$. Mit $(P(X))$ bezeichnen wir das Ideal von $P(X)$.
Wir wissen bereits, dass $\mathbb{K}[X]/(P(X))$ ein Ring ist. Zeige nun:

1. $\mathbb{K}[X]/(P(X))$ ist ein $\mathbb{K}$-Vektorraum mit Basis $\overline{1}, \ldots, \overline{X^{n-1}}$.
2. Sei $\lambda \in \mathbb{K}$, sodass $P(X) = X - \lambda$. Zeige, dass dann $\mathbb{K}[X]/(P(X)) \simeq \mathbb{K}$.
3. Sei $\mathbb{K} = \mathbb{R}$ und $P(X) = X^2 + 1$. Zeige, dass dann $\mathbb{R}[X]/(P(X)) \simeq \mathbb{C}$

Lösung:

1. Sei $f(X) = a_m X^m + a_{m-1} X^{m-1} + \ldots + a_1 X + a_0 \in \mathbb{K}[X]$, dann gibt es ein Polynom $g(X) \in \mathbb{K}[X]$ und geeignete Koeffizienten in $\mathbb{K}$, sodass

   $$f(X) = b_{n-1} X^{n-1} + \ldots + b_1 X + b_0 + g(X) P(X)$$

   Jedes Element in $\mathbb{K}[X]/(P(X))$ hat also einen Repräsentanten von Grad $n-1$ oder geringer. Wir können den Tupel der Koeffizienten als Zeilenvektor über $\mathbb{K}$ sehen, also

   $$b_{n-1} X^{n-1} + \ldots + b_1 X + b_0 \mapsto (b_{n-1}, \ldots, b_1, b_0) \in \mathbb{K}^n$$

   damit ist die Vektorraumstruktur offenbar.[a] Natürlich könnte man noch prüfen, dass wirklich alle Eigenschaften eines Vektorraums erfüllt werden. Wir müssen nun noch zeigen, dass $\overline{1}, \ldots, \overline{X^{n-1}}$ eine Basis bilden. Dazu zeigen wir, dass es ein linear unabhängiges Erzeugendensystem ist.

   - *Erzeugendensystem:* Das ist relativ klar. Sei $f \in \mathbb{K}[X]/(P(X))$, dann gilt

     $$f(X) \equiv a_{n-1} X^{n-1} + \ldots + a_1 X + a_0 \mod P(X) \equiv a_{n-1} \overline{X^{n-1}} + \ldots + a_1 \overline{X} + a_0 \mod P(X)$$

     also können wir jeden Vektor durch eine Linearkombination unserer Vektoren darstellen.

- *Lineare Unabhängigkeit:* Hierzu betrachten wir Koeffizienten $a_{n-1}, \dots, a_1, a_0$, sodass

$$\sum_{j=0}^{n-1} \alpha_j \overline{X^j} \equiv 0 \mod P(X) \tag{1}$$

  Angenommen die Linearkombination ist nicht trivial, es gibt also $a_j \neq 0$, dann existieren eindeutige $G(X), Q(X) \in \mathbb{K}[X]$, sodass:

$$\sum_{j=0}^{n-1} \alpha_j X^j = G(X) + P(X)Q(X)$$

  mit $-\infty \neq \deg(G(X)) < \deg(P(X))$, da wir in einem euklidischen Ring sind. Gleichzeitig gilt aber wegen Gleichung (1) auch, dass $G(X) = F(X)P(X)$ gelten muss. Da $\deg(F(X) \cdot P(X)) = \deg(F(X)) + \deg(P(X))$ gilt, folgt daraus $\deg(F(X)) = -\infty$, also auch $\deg(G(X)) = -\infty$, ein Widerspruch. Folglich gibt es also keine nichttriviale Linearkombination und die Vektoren sind linear unabhängig.

Mit diesen beiden Aussagen sehen wir, dass $\{\overline{X^{n-1}}, \dots, \overline{X}, \overline{1}\}$ eine Basis von $\mathbb{K}[X]/(P(X))$ bilden.

[a] Auch wenn die Schreibweise suggestiv ist, sehen wir hier noch nicht, dass unser Vektorraum n-dimensional ist. Es könnte ja theoretisch auch ein $n-k$-dimensionaler Unterraum sein.

2. Da $\deg(X - \lambda) = 1$ gilt, ist mit der ersten Teilaufgabe $\{\overline{1}\}$ eine Basis von $\mathbb{K}[X]/(P(X))$. Jeder n-dimensionale $\mathbb{K}$-Vektorraum ist isomorph zu $\mathbb{K}^n$, in diesem Fall ist $\mathbb{K}[X]/(P(X))$ also isomorph zu $\mathbb{K}$.

3. Wir betrachten die Abbildung

$$\begin{aligned} \varphi : \mathbb{C} &\to \mathbb{R}[X]/(X^2+1) \\ a + bi &\mapsto a + bX \end{aligned}$$

Diese Abbildung ist ein Ringhomomorphimus, denn für $a + bi, c + di \in \mathbb{C}$ gilt:

$$\begin{aligned} \varphi(a + bi + c + di) &= a + bX + c + dX = \varphi(a + bi) + \varphi(c + di) \\ \varphi((a + bi)(c + di)) &= \varphi((a - bd) + (bc + ad)i) \\ &= a - bd + (bc + ad)X \\ &\overset{(*)}{=} ac + bcX + adX + bdX^2 \\ &= (a + bX)(c + dX) = \varphi(a + bi)\varphi(c + di) \end{aligned}$$

, wobei wir in $(*)$ verwendet haben, dass in unserem Faktorring $X^2 + 1 = 0$, also auch $X^2 = -1$ gilt. Somit ist $-bd = bdX^2$. Betrachten wir $\mathbb{C}$ als $\mathbb{R}$-Vektorraum, dann gilt weiterhin die Verträglichkeit der Abbildung mit der Vektorraumaddition, für ein $\lambda \in \mathbb{R}$ gilt allerdings auch

$$\begin{aligned} \varphi(\lambda(a + bi)) &= \varphi(\lambda a + \lambda bi) \\ &= \lambda a + \lambda bX \\ &= \lambda(a + bX) = \lambda\varphi(a + bi) \end{aligned}$$

also ist die Abbildung auch ein $\mathbb{R}$-Vektorraumhomomorphismus. Injektivität und Surjektivität sind Eigenschaften einer Abbildung zwischen Mengen. Zeigen wir, dass φ injektiv ist, indem wir die Eigenschaft als Ringhomomorphismus verwenden, dann ist φ also auch als Vektorraumhomomorphismus injektiv. Wir wissen, dass (Ring-)Homomorphismen aus Körpern heraus immer injektiv sind. Da die Dimension von $\mathbb{C}$ als $\mathbb{R}$-Vektorraum mit der $\mathbb{R}$-Dimension von $\mathbb{R}[x]/(x^2+1)$ übereinstimmt folgt daraus sofort auch, dass φ (weil φ auch ein Vektorraumhomomorphismus ist) surjektiv ist. Also gilt $\mathbb{C} \simeq \mathbb{R}[X]/(X^2+1)$.

Aufgabe 4

1. Sei $\mathbb{K}$ ein Körper und $P_1(X), \ldots, P_m(X) \in \mathbb{K}[X]$ paarweise koprime Polynome. Zeige
$$\mathbb{K}[X]/(P_1(X), \ldots P_m(X)) \simeq \mathbb{K}[X]/(P_1(X)) \times \ldots \times \mathbb{K}[X]/(P_m(X))$$
2. Zeige $\mathbb{R}[X]/(X^2-1) \simeq \mathbb{R}^2$

Lösung:

1. Diese Aufgabe ist analog zu Aufgabe 1.1 zu lösen. Koprime Polynome sind teilerfremde Polynome, also enthalten die Faktorisierungen in irreduzible Polynome keine gemeinsamen Faktoren. Wir schreiben also
$$P_j(X) = q_{j,1}^{s_{j,1}}(X) \cdot \ldots \cdot q_{j,r_j}^{s_{j,r_j}}(X)$$
als die eindeutige Zerlegung von P_j in irreduzible Faktoren $q_{j,k}$ mit Vielfachheit $s_{j,k}$ und erhalten insgesamt
$$\mathbb{K}[X]/(P_1 \cdot \ldots \cdot P_m) \simeq \mathbb{K}[X]/\left(q_{1,1}^{s_{1,1}}(X) \cdot \ldots \cdot q_{1,r_1}^{s_{1,r_1}}(X) \cdot q_{2,1}^{s_{2,1}}(X) \cdot \ldots \cdot q_{m,r_m}^{s_{m,r_m}}(X)\right)$$
und $\forall j \neq j', k \neq k'$ gilt wegen der Teilerfremdheit $q_{j,k} \neq q_{j',k'}$. Wir können also wie in Aufgabe 1 vorgehen und betrachten zuerst nur den Faktorring über $q^r \cdot p^s$ für zwei beliebige irreduzible Polynome $q, p \in \mathbb{K}[X]$. Wir betrachten also die Abbildung
$$\varphi : \mathbb{K}[X]/(q^r(X) \cdot p^s(X)) \to \mathbb{K}[X]/(q^r(X)) \times \mathbb{K}[X]/(p^s(X))$$
$$f + (q^r \cdot p^s)\mathbb{K}[X] \mapsto (f + q^r\mathbb{K}[X], f + p^s\mathbb{K}[X])$$
Wir zeigen analog, dass die Abbildung ein Homomorphismus (sowohl von Ringen, als auch von Vektorräumen) ist. Mit Aufgabe 3 sehen wir, dass die beiden Ringe links und rechts als Vektorräume gesehen dieselbe Dimension haben. Wir verwenden, dass φ ein Homomorphismus von Vektorräumen ist und sehen, dass es erneut ausreichend ist Injektivität zu zeigen indem wir zeigen, dass der Kern trivial ist (als Übung überlassen) und erhalten Bijektivität sofort dazu. φ ist also als Vektorraumhomomorphismus bijektiv - da Bijektivität aber eine Eigenschaft von Abbildungen zwischen Mengen ist, ist φ damit natürlich auch als Ringhomomorphismus bijektiv und damit sind die beiden Ringe isomorph. Der Rest der Aussage folgt mit vollständiger Induktion.

Streng genommen steht in der Aufgabe nicht, welche Art von Isomorphie man zeigen soll. Ist man hier nur an der Vektorraumisomorphie interessiert, gibt es hier noch einen weiteren Weg, die Aufgabe zu lösen. Da $\mathbb{K}$ ein Körper ist, ist $\mathbb{K}[X]$ ein Integritätsbereich, also gilt

$$\deg(P_1 \cdot \ldots \cdot P_m) = \deg(P_1) + \ldots + \deg(P_m)$$

also haben beide Ringe als Vektorraum die gleiche Dimension. Damit sind sie isomorph als Vektorräume. Da wir hier aber keine Abbildung konstruiert haben, können wir hier nicht schließen, dass beide Vektorräume auch als Ringe isomorph sind.[a]

[a] Zu zeigen, dass ein Ringhomomorphismus existiert, reicht hier nicht aus. Zwischen isomorphen Vektorräumen kann es Homomorphismen geben, die keine Isomorphismen sind, z.B. die Abbildung $x \mapsto 0$.

2. Es gilt $X^2 - 1 = (X-1)(X+1)$, damit gilt

$$\mathbb{R}[X]/(X^2-1) \simeq \mathbb{R}[X]/(X-1) \times \mathbb{R}[X]/(X+1) \simeq \mathbb{R} \times \mathbb{R}$$

wobei wir Aufgabe 3.2 und 4.1 verwendet haben.