Lineare Algebra 2 — Lösung zu Übungsblatt 1

Sommersemester 2020

AOR Dr. D. Vogel
P. Gräf, R. Steingart *Abgabe:* Do 07.05.2020 um 9:15 Uhr

Wie in der Vorlesung sind im Folgenden alle Ringe kommutativ mit Eins.

4. Aufgabe: (*2+2+2 Punkte, Polynomringe über allgemeinen Ringen*) Sei R ein Ring. Ein *Polynom* mit Koeffizienten in R ist ein Ausdruck

$$f = f(t) = a_0 + a_1 t + \cdots + a_n t^n; \quad a_j \in R.$$

Die Menge der Polynome mit Koeffizienten in R wird mit $R[t]$ bezeichnet. Ist in der obigen Darstellung $a_n \neq 0$, so heißt n der *Grad* von f (Notation $\deg(f)$). Wir haben eine natürliche Inklusion von $R \hookrightarrow R[t]$, die $r \in R$ das konstante Polynom r ($a_0 = r$, $a_i = 0$ für $i \geq 1$) zuordnet. Seien $f = \sum_{i=0}^{\infty} a_i t^i$ und $g = \sum_{i=0}^{\infty} b_i t^i$ in $R[t]$. Wir definieren

$$f + g := \sum_{i=0}^{\infty} (a_i + b_i) t^i \quad \text{und} \quad f \cdot g := \sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} a_j b_{i-j} \right) t^i.$$

Dann ist $(R[t], +, \cdot, 0)$ ein Ring. Die Inklusion $R \hookrightarrow R[t]$ ist ein Ringhomomorphismus.

(a) Man zeige: Ist R nullteilerfrei, so gilt $R[t]^\times = R^\times$.

(b) Man zeige anhand einen Gegenbeispiels, dass die Aussage aus (a) für nicht nullteilerfreie Ringe im Allgemeinen falsch ist.

(c) Man gebe einen Ring R und ein Polynom $f \in R[t] \setminus \{0\}$ an mit

$$\#\{r \in R \mid f(r) = 0\} > \deg(f).$$

Bemerkung: Ist R ein Körper, so gibt es nach Korollar 4.10 aus der Linearen Algebra 1 kein solches Polynom.

Lösung:

(a) Seien $f = \sum_{i=0}^{\infty} a_i t^i$ und $g = \sum_{i=0}^{\infty} b_i t^i$ zwei von 0 verschiedene Polynome in $R[t]$ mit $n = \deg(f)$ und $m = \deg(g)$. Dann gilt $a_n, b_m \neq 0$. Da R nullteilerfrei ist, ist dann auch $a_n b_m \neq 0$. Es ist

$$f \cdot g = \sum_{i=0}^{n+m} \left(\sum_{j=0}^{i} a_j b_{i-j} \right) t^i.$$

Für den $(n+m)$-ten Koeffizienten gilt

$$\sum_{j=0}^{n+m} a_j b_{n+m-j} = a_0 \underbrace{b_{n+m}}_{=0} + a_1 \underbrace{b_{n+m-1}}_{=0} + \ldots + a_{n-1} \underbrace{b_{m+1}}_{=0} + a_n b_m + \underbrace{a_{n+1}}_{=0} b_{m-1} + \ldots + \underbrace{a_{n+m}}_{=0} b_0 = a_n b_m \neq 0.$$

Insbesondere folgt $\deg(fg) = n + m = \deg(f) + \deg(g)$.

Sei nun $f \in R[X]^\times$ eine Einheit. Dann ist $f \neq 0$ und es existiert ein $g \in R[X], g \neq 0$ mit $fg = 1$. Insbesondere ist $0 = \deg(fg) = \deg(f) + \deg(g)$, d.h. $\deg(f) = \deg(g) = 0$.
f und g sind daher konstante Polynome und es gilt $fg = 1$. Folglich ist $f \in R^\times$.
Umgekehrt existiert für $f \in R^\times$ ein $g \in R^\times$ mit $fg = 1$. Man kann f, g als konstante Polynome in $R[X]$ auffassen. Da die Inklusion ein Homomorphismus ist, gilt auch in $R[X]$: $fg = 1$, d.h. $f \in R[X]^\times$.

(b) Sei $R = \mathbb{Z}/4\mathbb{Z}$. R ist nicht nullteilerfrei, da 4 keine Primzahl ist. Es gilt

$$(\overline{2}t + \overline{3})^2 = \overline{4}t^2 + \overline{12}t + \overline{9} = \overline{1}.$$

Damit ist $\overline{2}t + \overline{3} \in R[t]^\times$, aber offensichtlich ist $\overline{2}t + \overline{3} \notin R^\times$.

(c) Sei $R = \mathbb{Z}/4\mathbb{Z}$ und $f = \overline{2}t$. Offensichtlich ist $f \neq 0$, denn $f(\overline{1}) = \overline{2} \neq \overline{0}$. Es ist

$$f(\overline{0}) = \overline{0} \text{ und } f(\overline{2}) = \overline{0}.$$

Damit ist $\#\{r \in R \mid f(r) = 0\} \geq 2 > 1 = \deg(f)$.

5. Aufgabe: *(1,5+1,5+1,5+1,5 Punkte, Komplexe Zahlen als Faktorring)* Sei $\varphi\colon \mathbb{R}[t] \to \mathbb{C}$ die Abbildung

$$f = a_0 + a_1 t + \cdots + a_n t^n \mapsto f(i) = a_0 + a_1 i + \cdots + a_n i^n.$$

Hierbei bezeichnet $i \in \mathbb{C}$ die imaginäre Einheit mit $i^2 = -1$. Man zeige:

(a) φ ist ein surjektiver Ringhomomorphismus.

(b) Es ist $t^2 + 1 \in \ker(\varphi)$ und für alle $f \in \mathbb{R}[t] \setminus \{0\}$ mit $\deg(f) < 2$ gilt $\varphi(f) \neq 0$.

(c) Es gilt: $\ker(\varphi) = (t^2 + 1)$.
Hinweis: Man verwende Division mit Rest, Satz 4.6 aus der Linearen Algebra 1.

(d) Es gilt: Die Ringe $\mathbb{R}[t]/(t^2 + 1)$ und $\mathbb{C}$ sind isomorph, und $(t^2 + 1) \subseteq \mathbb{R}[t]$ ist ein maximales Ideal.

Lösung:

(a) φ ist ein Homomorphismus, denn für $f, g \in \mathbb{R}[t]$ mit $f = \sum_{k=0}^\infty a_k t^k$ und $g = \sum_{k=0}^\infty b_k t^k$ gilt:

- $\varphi(f + g) = \varphi(\sum_{k=0}^\infty (a_k + b_k) t^k) = \sum_{k=0}^\infty (a_k + b_k) i^k = \sum_{k=0}^\infty a_k i^k + \sum_{k=0}^\infty b_k i^k = \varphi(f) + \varphi(g)$
- $$\begin{aligned}\varphi(f \cdot g) &= \varphi\left(\sum_{k=0}^\infty \left(\sum_{j=0}^k a_j b_{k-j}\right) t^k\right) = \sum_{k=0}^\infty \left(\sum_{j=0}^k a_j b_{k-j}\right) i^k \\ &= \sum_{k=0}^\infty a_k i^k \cdot \sum_{k=0}^\infty b_k i^k = \varphi(f) \cdot \varphi(g)\end{aligned}$$
- $h \equiv 1 \implies \varphi(h) = h(i) = 1$

φ ist surjektiv, denn: Für $z = a + bi \in \mathbb{C}$ wähle $f = a + bt \in \mathbb{R}[t]$. Dann gilt

$$\varphi(f) = f(i) = a + bi = z.$$

(b) Zunächst gilt $\varphi(t^2 + 1) = i^2 + 1 = -1 + 1 = 0$, also ist $t^2 + 1 \in \ker(\varphi)$. Ist nun $f = a_0 + a_1 t$ ein Polynom in $\mathbb{R}[t]$ mit $\deg(f) < 2$, so gilt:

$$\varphi(f) = 0 \;\Leftrightarrow\; a_0 + a_1 i = 0 \;\Leftrightarrow\; a_0 = a_1 = 0 \;\Leftrightarrow\; f = 0,$$

d.h. $\varphi(f) \neq 0$ für $f \in \mathbb{R}[t] \setminus \{0\}$.

(c) Für $f \in (t^2 + 1)$ existiert ein $r \in \mathbb{R}[t]$ mit $f = r(t^2 + 1)$. Dann ist

$$\varphi(f) \overset{(a)}{=} \varphi(r)\varphi(t^2 + 1) \overset{(b)}{=} \varphi(r) \cdot 0 = 0.$$

Damit gilt $(t^2 + 1) \subseteq \ker(\varphi)$.
Sei nun umgekehrt $f \in \ker(\varphi)$, i.e. $\varphi(f) = 0$. Nach dem Satz über die Polynomdivision existieren eindeutig bestimmte Polynome $q, r \in \mathbb{R}[t]$ mit $\deg(r) < 2$ und $f = q(t^2 + 1) + r$. Es ist dann

$$0 = \varphi(f) = \varphi(q)\varphi(t^2 + 1) + \varphi(r) = \varphi(r).$$

Nach (b) ist $\varphi(r) \neq 0$ für $r \neq 0$. Daher folgt direkt $r = 0$ sowie $f = q(t^2 + 1) \in (t^2 + 1)$ und wir erhalten $\ker(\varphi) \subseteq (t^2 + 1)$.

(d) Nach (a) und (c) gilt $\mathrm{im}(\varphi) = \mathbb{C}$ und $\ker(\varphi) = (t^2 + 1)$. Durch Anwendung des Homomorphiesatzes auf φ erhalten wir einen Ringisomorphismus

$$\mathbb{R}[t]/(t^2 + 1) = \mathbb{R}[t]/\ker(\varphi) \cong \mathrm{im}(\varphi) = \mathbb{C}.$$

Da $\mathbb{C}$ ein Körper ist, folgt bereits, dass $\mathbb{R}[t]/(t^2 + 1)$ ein Körper sein muss. Nach Bem. 1.23 aus der Vorlesung ist $(t^2 + 1)$ dann schon ein maximales Ideal.

6. Aufgabe: *(2+2+2 Punkte, Radikalideale)* Sei R ein Ring und $I \subseteq R$ ein Ideal. Wir definieren

$$\sqrt{I} := \{r \in R \mid \text{es gibt } n \in \mathbb{N} \text{ mit } r^n \in I\}.$$

(a) Man zeige: $\sqrt{I}$ ist ein Ideal in R mit $I \subseteq \sqrt{I}$.

(b) Man zeige: Ist I ein Primideal, so gilt $\sqrt{I} = I$.

(c) Man gebe ein Beispiel für einen Ring R und ein Ideal $I \subseteq R$ an, sodass I kein Primideal ist, aber $\sqrt{I} = I$ gilt.

Lösung:

(a) Wir prüfen die Axiome I1-I3, um zu zeigen dass $\sqrt{I} \subset R$ Ideal ist:

I1: $0 \in \sqrt{I}$, da $0^1 = 0 \in I$.

I2: Seien $a, b \in \sqrt{I} \Rightarrow \exists n, m \in \mathbb{N} : a^n, b^m \in I$. Mit dem binomischen Lehrsatz gilt

$$(a + b)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} a^{(n+m)-k} b^k.$$

Die einzelnen Summanden liegen in I, da entweder $a^{(n+m)-k} \in I$ für $k \leq m$ oder $b^k \in I$ für $k > m$. Damit liegt $a + b$ in $\sqrt{I}$.

I3: Sei $r \in R, a \in \sqrt{I}$. Es existiert ein $n \in \mathbb{N}$, sodass $a^n \in I$. Es gilt $(ra)^n = r^n a^n \in I$ und damit $ra \in \sqrt{I}$.

Außerdem gilt $I \subset \sqrt{I}$, denn für Elemente aus I können wir $n = 1$ wählen.

(b) Sei I ein Primideal, d.h. es gilt $ab \in I \Rightarrow a \in I$ oder $b \in I$. Zu zeigen ist $\sqrt{I} = I$, also die Inklusion $\sqrt{I} \subset I$, da $I \subset \sqrt{I}$ nach a) bereits gilt. Sei also $r \in \sqrt{I}$. Das heißt es gibt ein $n \in \mathbb{N}$ mit $r^n \in I$. Man kann schreiben $r^n = r^{n-1}r$. Ein Faktor muss in I liegen, da I Primideal ist. Wenn wir annehmen, dass r nicht in I ist, so muss es aber r^{n-1} sein. Auch r^{n-1} können wir wieder in zwei Faktoren zerlegen und das sukzessive fortführen, bis wir $r^2 = rr$ haben und folgern können, dass r bereits Element von I gewesen sein muss.

(c) Mögliche Beispiele:

- $I = R$, da wir den ganzen Ring in der Definition eines Primideals explizit ausgenommen haben
- $I = 6\mathbb{Z}$ (oder andere Schnitte von Primidealen). Begründung: Sei $r \in \sqrt{I} \Rightarrow \exists n \in \mathbb{N}$ mit $r^n \in I = 6\mathbb{Z}$, also $r^n = 6z, z \in \mathbb{Z}$. D.h. $6 \mid r^n \Rightarrow 2 \mid r^n$ und $3 \mid r^n \Rightarrow r^n \in 2\mathbb{Z}$ und $r^n \in 3\mathbb{Z}$. Dies sind Primideale, also folgt mit Teil b): $r \in 2\mathbb{Z}$ und $r \in 3\mathbb{Z} \Rightarrow r \in 2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$.

7. Aufgabe: *(2+3+1 Punkte, Ideale im Faktorring)* Ziel dieser Aufgabe ist es Bemerkung 1.14 aus der Vorlesung zu beweisen. Seien dazu R ein Ring, $I \subseteq R$ ein Ideal und $\pi\colon R \to R/I$ die kanonische Projektion $r \mapsto \bar{r} = r + I$. Wir definieren Abbildungen Φ und Ψ wie folgt:

$$\left\{\text{Ideale in } R/I\right\} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \left\{\text{Ideale } \tilde{I} \text{ in } R \text{ mit } I \subseteq \tilde{I}\right\}$$
$$J \mapsto \pi^{-1}(J)$$
$$\pi(J) \leftarrow\!\shortmid J$$

(a) Man zeige, dass die Abbildungen Φ und Ψ wohldefiniert und inklusionserhaltend sind.

(b) Man zeige, dass die Abbildungen Φ und Ψ invers zueinander sind, es handelt sich also um inklusionserhaltende Bijektionen.

(c) Man bestimme für $R = \mathbb{Z}$ und $I = (15)$ alle Ideale in in R/I.

Lösung:

(a) Für die Wohldefiniertheit muss gezeigt werden, dass die Abbildungen Φ und Ψ in die entsprechenden Wertebereiche abbilden. Da π ein surjektiver Ringhomomorphismus ist (1.10), sind $\pi^{-1}(J)$ und $\pi(J)$ wieder Ideale (1.8). Es gilt $I \subset \pi^{-1}(J)$, da $\pi(a) = 0 \in J$ für alle $a \in I$.

Die beiden Abbildungen sind außerdem inklusionserhaltend:

- (Φ): Sei $J_1 \subset J_2$ in R/I. Sei $r \in \Phi(J_1) = \pi^{-1}(J_1) \Rightarrow \pi(r) \in J_1 \subset J_2 \Rightarrow r \in \pi^{-1}(J_2) = \Phi(J_2)$.
- (Ψ): Sei $J_1 \subset J_2$ in $R \Rightarrow \Psi(J_1) = \pi(J_1) \subset \pi(J_2) = \Psi(J_2)$.

(b) Die beiden Abbildungen Φ und Ψ sind invers zueinander:

- ($\Phi \circ \Psi = id$): Sei $J \subset R$ Ideal mit $I \subset J$. Dann gilt $\Phi \circ \Psi(J) = \Phi(\pi(J)) = \pi^{-1}(\pi(J))$. Sei $r \in \pi^{-1}(\pi(J)) \Leftrightarrow \pi(r) \in \pi(J) \Leftrightarrow r + I \in J + I$. Da $I \subset J$ ist dies äquivalent zu $r \in J$. Also $\Phi \circ \Psi(J) = \pi^{-1}(\pi(J)) = J$.
- ($\Psi \circ \Phi = id$): Sei $J \subset R/I$ Ideal. Es gilt $\Psi \circ \Phi(J) = \Psi(\pi^{-1}(J)) = \pi(\pi^{-1}(J))$. Nach Definition des Urbildes gilt $\pi(\pi^{-1}(J)) \subset J$. Sei umgekehrt $x \in J$. Da π surjektiv ist, finden wir $r \in R$ mit $\pi(r) = x$, also ist $r \in \pi^{-1}(J)$ und $x = \pi(r) \in \pi(\pi^{-1}(J))$. Also $\Psi \circ \Phi(J) = J$.

(c) Mithilfe der Abbildungen Φ und Ψ können wir nun im konkreten Fall $R = \mathbb{Z}, I = (15)$ die Ideale in R/I bestimmen. Diese korrespondieren nämlich zu Idealen in $R = \mathbb{Z}$, die $I = (15)$ enthalten. Aus der Vorlesung wissen wir, dass alle Ideale in $\mathbb{Z}$ von der Form $n\mathbb{Z}, n \in \mathbb{Z}$ sind. Es gilt $(15) = 15\mathbb{Z} \subset n\mathbb{Z} \Leftrightarrow n \mid 15 \Leftrightarrow n \in \{\pm1, \pm3, \pm5, \pm15\}$. Durch Anwenden von Ψ auf die Ideale $n\mathbb{Z}$ erhalten wir folgende vier Ideale von R/I: $\mathbb{Z}/(15) \cong 1\mathbb{Z}/(15) \cong (-1)\mathbb{Z}/(15)$, $3\mathbb{Z}/(15) \cong (-3)\mathbb{Z}/(15)$, $5\mathbb{Z}/(15) \cong (-5)\mathbb{Z}/(15)$, $15\mathbb{Z}/(15) \cong (-15)\mathbb{Z}/(15) \cong (\bar{0})$.

Die Übungsblätter sowie weitere Informationen zur Vorlesung sind über **MaMpf** abrufbar.