Lineare Algebra 1 Hausaufgabenblatt Nr. 4

Jun Wei Tan*

Julius-Maximilians-Universität Würzburg

(Dated: November 17, 2023)

Problem 1. Es sei K ein Körper. Ferner seien $a, b \in K[t] \setminus \{0\}$ Polynome.

Wir definieren $r_0 := a, r_1 := b$ und definieren für $k \in \mathbb{N}$ q_k und r_{k+1} als Polynome, die

$$r_{k-1} = q_k r_k + r_{k+1} \qquad \deg(r_{k+1}) < \deg(r_k)$$

erfüllen, falls $r_k \neq 0$ und ansonsten definieren wir $r_{k+1} = r_k = 0$.

(a) Zeigen Sie: Es gibt ein minimales $k_0 \in \mathbb{N}$, sodass $r_k = 0$ für alle $k > k_0$.

(b) Zegen Sie: Mit dieser Wahl ist $r_{k_0} \neq 0$ und r_{k_0} ist ein gemeinsamer Teiler von a und b.

(c) Zeigen Sie: Ist $s \in K[t]$ ein gemeinsamer Teiler von a und b, dann ist s auch ein Teiler von r_{k_0}.

Proof. (a) Es gilt $\deg(r_k) < \deg(r_k)$, also die Folge $\deg(r_k)$ ist streng monoton fallend. Weil es nur endliche Möglichkeiten k für die Grad eines Polynomes mit $k < \deg(b)$ gibt, muss es ein Zahl k_0' geben, mit $\deg(r_{k_0'}) = -\infty$.

(Die Möglichkeiten sind $\{-\infty, 0, 1, \ldots, \deg(b)\}$.)

$\deg(r_{k_0}) = -\infty$ genau dann, wenn $r_{k_0} = 0$. Es folgt per Definition, $r_{k_0+1} = 0$ und $r_k = 0 \; \forall k \geq k_0$ per Induktion.

Weil $\{0, 1, \ldots, k_0'\}$ endlich ist, gibt es ein minimales Zahl k_0 mit die gewünsche Eigenschaft.

(b) Mit dieser Wahl ist $r_{k_0} \neq 0$.

* jun-wei.tan@stud-mail.uni-wuerzburg.de

Sonst wäre es ein Widerspruch, weil k_0 nicht die kleinste Zahl mit diese Eigenschaft wäre. Falls $r_{k_0} = 0$, wäre $k_0 - 1$ eine kleine Zahl mit die gewünschte Eigenschaft.

(i) Wir beweisen zuerst die folgende Behauptung:

> Sei p ein gemeinsamer Teiler von r_k und r_{k+1}. Dann ist p auch ein gemeinsamer Teiler von r_k und r_{k-1}.

Per Definition teilt p r_k. Wir wissen auch, dass

$$r_{k-1} = q_k r_k + r_{k+1}.$$

Weil p teilt r_k, teilt p $q_k r_k$ auch. Da p teilt auch r_{k+1}, teilt p $q_k r_k + r_{k+1}$, also p teilt r_{k-1}. Dann ist p ein gemeinsamer Teiler von r_k und r_{k-1}.

(ii) Sei p ein gemeinsamer Teiler von r_{k-1} und $r_k, k \leq k_0$. Dann ist p auch ein gemeinsamer Teiler von a und b.

Wir beweisen es per Induktion. Für $k = 1$ ist es klar, dass alle gemeinsamer Teiler von a und b auch gemeinsamer Teiler von a und b sind.

Jetzt nehmen wir an, dass es für eine beliebige $\mathbb{N} \ni k < k_0$ gilt, dass alle gemeinsamer Teiler von r_k und r_{k-1} auch gemeinsamer Teiler von a und b sind.

Jetzt betrachten wir r_k und r_{k+1}. Sei p ein gemeinsamer Teiler von r_k und r_{k+1}. Aus (i) folgt, dass p auch ein Teiler von r_k und r_{k-1} ist. Per Induktionvoraussetzung ist p auch ein gemeinsamer Teiler von a und b.

(iii) Insbesondere gilt, dass alle gemeinsamer Teiler p von r_{k_0} und r_{k_0-1} auch gemeinsamer Teiler von a und b sind.

(iv) In (a) haben wir schon bewiesen, dass r_{k_0} ein Teiler von r_{k_0-1} ist. Daraus folgt, dass r_{k_0} ein gemeinsamer Teiler von r_{k_0} und r_{k_0-1} ist. Es folgt, dass r_{k_0} ein gemeinsamer Teiler von a und b ist.

(c) Der Beweis läuft ähnlich:

(i) Wir beweisen per Induktion:

> Sei p ein gemeinsamer Teiler von a und b. p ist dann ein gemeinsamer Teiler von r_k und r_{k-1} für alle $k \in \{0, 1, \ldots, k_0\}$.

(ii) Induktionsvoraussetzung: Wir nehmen an, dass es für beliebige $\mathbb{N} \ni k \leq k_0 - 1$, dass alle gemeinsamer Teiler von a und b auch gemeinsamer Teiler von r_k und r_{k-1} sind.

(iii) Wir betrachten p, was ein gemeinsamer Teiler von a und b ist, also per Induktionsvoraussetzung ist p ein gemeinsamer Teiler von r_k und r_{k-1}.

Es gilt $r_{k+1} = r_{k-1} - q_k r_k$, also weil p r_k teilt, teilt p $q_k r_k$. Es folgt, dass p teilt $r_{k-1} - q_k r_k$, und p teilt r_{k+1}. Also p ist ein gemeinsamer Teiler von r_{k+1} und r_k.

Insbesondere gilt, dass wenn $s \in K[t]$ ein gemeinsamer Teiler von a und b ist, ist s ein gemeinsamer Teiler von r_{k_0} und r_{k_0-1}, also s ist ein Teiler von r_{k_0}. $\square$

Problem 2. (a) Zeigen Sie: Ist K ein endlicher Körper, so gibt es ein Polynom $p \neq 0$, das alle $x \in K$ als Nullstelle hat. Folgern Sie daraus, dass die Abbildung $K[t] \to \mathrm{Abb}(K, K), f \to (x \to f(x))$ in diesem Fall nicht injektiv ist.

(b) Zeigen Sie: Ist $p \in K[t]$ ein Polynom vom Grad 0, 1, 2 oder 3, das keine Nullstelle in K hat, dann hat von zwei Polynomen f, g mit $f \cdot g = p$ mindestens eines Grad 0.

(c) Bestimmen Sie mit dem vietaschen Nullstellensatz alle rationalen Nullstellen von

$$q = 99 \cdot t^3 - 63 \cdot t^2 - 44 \cdot t + 28 \in \mathbb{Q}[t].$$

(d) Beweisen Sie, dass das Polynom $t^8 - 2 \in \mathbb{Q}[t]$ keine rationalen Nullstellen hat.

(e) Es seien $f = (2 + 3i)X^7 - 5$ und $g = X^2 - 2i$ in $\mathbb{C}[X]$ gegeben. Bestimmen Sie wie im Existenzbeweis von Satz 2.4.26 die Polynome $q, r \in \mathbb{C}[X]$ mit $\deg(r) < \deg(g)$ und

$$f = q \cdot g + r.$$

Proof. (a) Wir beweisen es konstruktiv. Sei $p = \prod_{r \in K}(x - r)$. Es gilt, für alle $x \in K$, dass $x - x = 0$, also $p(x) = 0$. Aber $p \neq 0$, z.B. ist das Koeffizient $a_n = 1$, wobei $n = |K|$.

Wir wissen, dass die Abbildung das konstruierte Polynom auf die Nullfunktion abbildet. Aber die Abbildung bildet auch das Nullpolynom auf die Nullfunktion ab. Also wir haben $K[t] \ni 0 \neq p \in K[t]$, aber die Abbildung bildet 0 und p auf die gleiche Funktion, also es ist nicht injektiv.

(b) Es gilt

$$\deg(p) = \deg(f) + \deg(g),$$

also es gibt nur zwei Möglichkeiten für $\deg(f)$ und $\deg(g)$: Entweder haben wir $0 + 3 = 3$ oder $1 + 2 = 3$.

Sei $\deg(f) = 1$ und $\mathrm{def}(g) = 2$, mit $p = f \cdot g$. Per Definition ist $f(t) = a_0 + a_1 t, a_0, a_1 \in K$. Sei $t = -a_1^{-1} a_0 \in K$. Es gilt $\tilde{f}(t) = a_0 - a_1 a_1^{-1} a_0 = 0$, also t ist eine Nullstelle von f.

Es folgt daraus, dass t ist eine Nullstelle von p, ein Widerspruch zu die Annahme, dass p keine Nullstellen hat.

Jetzt bleibt nur eine Möglichkeit, dass von f, g mindestens eines (eigentlich genau eine) Grad 0 hat.

(c) Für alle rationale Nullstellen $a/b, a \in \mathbb{N} \cup \{0\}, b \in \mathbb{Z}$, a, b teilerfremd gilt

$$a|28 \qquad b|99.$$

Weil $28 = 2^2 \times 7$ und $99 = 3^2 \times 11$, sind die Möglichkeiten dafür:

$$a \in \{1, 2, 4, 7, 14, 28\}$$

$$b \in \{1, 3, 9, 11, 33, 99\}$$

(d) Wir verwenden Satz 2.4.37. Sei $x = \frac{p}{q} \in \mathbb{Q}$, $p, q \in \mathbb{Z}, q > 0$ teilerfremd, eine Nullstelle von $t^8 - 2$. Dann gilt

$$p| - 2 \qquad q|1,$$

also $q = 1$ und $p \in \{-2, -1, 0, 1, 2\}$, dann $x \in \{-2, -1, 0, 1, 2\}$. Aber für keine mögliche x gilt $x^8 - 2 = 0$, also $t^8 - 2 \in \mathbb{Q}[t]$ hat keine rationale Nullstellen.

(e)

$$\begin{aligned}(2+3i)X^7-5 =& (X^2-2i)((2+3i)X^5-(6-4i)X^3\\ &-(8+12i)X)+\underbrace{(24-16i)X-5}_{r}.\end{aligned}$$

□

Problem 3. Beweisen oder widerlegen Sie folgende Behauptungen:

(a) $\mathbb{R}$ wird mit der gewöhnlichen Addition und Multiplikation ein $\mathbb{Q}$-Vektorraum.

(b) $\mathbb{Z}$ wird mit der gewöhnlichen Addition und der Multiplikation $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z} : \overline{0} \cdot z = 0, \overline{1} \cdot z = z$ zu einem $\mathbb{Z}/2\mathbb{Z}$-Vektorraum.

(c) Der Ring $\mathbb{C} \times \mathbb{R}$ wird mit der Multiplikation $a \cdot (z, r) = (az, ar)$ zu einem $\mathbb{R}$-Vektorraum.

(d) Der Ring $\mathbb{C} \times \mathbb{R}$ wird mit der Multiplikation $a \cdot (z, r) = (az, ar)$ zu einem $\mathbb{C}$-Vektorraum.

(e) Jeder $\mathbb{C}$-Vektorraum ist mit der entsprechend eingeschränkten Multiplikation auch ein $\mathbb{R}$-Vektorraum.

Proof. (a) Wahr. Wir wissen, dass $(\mathbb{R}, +, 0)$ eine abelsche Gruppe ist.

Die andere Gruppenaxiome folgen aus die analoge Axiome für Addition und Multiplikation in $\mathbb{R}$, wenn man $(\mathbb{Q}, +, \cdot, 0, 1)$ als Unterring von $(\mathbb{R}, +, \cdot, 0, 1)$ betrachtet.

(b) Falsch. Das Distributivgesetz wird verletzt. Sei $a \in \mathbb{Z}, a \neq 0$ und daher $a + a \neq 0$. Es gilt

$$\begin{aligned}a + a =& \overline{1} \cdot a + \overline{1} \cdot a\\ \neq& (\overline{1} + \overline{1})a\\ =& \overline{0} \cdot a\\ =& 0\end{aligned}$$

(c) Wahr. Es folgt ähnlich zu (a):

Wir haben $+, \cdot : \mathbb{C} \to \mathbb{C}$. Wir wissen, dass $(\mathbb{R}, +|_{\mathbb{R}\times\mathbb{R}}, \cdot|_{\mathbb{R}\times\mathbb{R}}, 0, 1)$ ein Unterring ist. Daraus folgt, dass $\mathbb{C} \times \mathbb{R}$ mit der Multiplikation $a \cdot (z, r) = (az, ar)$ ein $\mathbb{R}$-Vektorraum ist.

(d) Falsch. Es gilt, z.B. $(1,1) \in \mathbb{C} \times \mathbb{R}$, $i \in \mathbb{C}$, aber

$$i \cdot (1,1) = (i,i) \notin \mathbb{C} \times \mathbb{R}.$$

$\square$

Problem 4. Es sei $(V, +)$ eine abelsche Gruppe. Zeigen Sie:

(a) Die Menge End (V) aller Homomorphismen von $V \to V$ bildet mit den Verknüpfungen

$$\oplus : \mathrm{End}(V) \times \mathrm{End}(V) \to \mathrm{End}(V), f \oplus g := (V \to V, x \to f(x) + g(x))$$

und $\circ$ der gewöhnlichen Hintereinanderausführung von Abbildungen, einen Ring mit 1.

(b) Enthält End(V) einen Körper K, dann ist $(V, +)$ mit der skalaren Multiplikation $k \cdot v := k(v)$ ein K-Vektorraum.

Proof. (a) (i) Wir wissen, weil $(V, +)$ abelsch ist, dass $(\mathrm{End}(V), \oplus)$ auch eine abelsche Gruppe ist.

(ii) Wir wissen auch, dass Verkettung von Funktionen assoziativ ist.

(iii) Distributivgesetz: Sei $f, g, h \in \mathrm{End}(V)$. Es gilt, für beliebige $x \in V$,

$$\begin{aligned} [f \circ (g \oplus h)]\,(x) =& f(g(x) + h(x)) \\ =& f(g(x)) + f(h(x)) \qquad f \text{ ist ein Homomorphismus} \\ =& (f \circ g)(x) + (f \circ h)(x) \\ =& \left[(f \circ g) \oplus (f \circ h)\right](x) \end{aligned}$$

Weil x beliebig war, ist $f \circ (g \oplus h) = (f \circ g) \oplus (f \circ h)$

(iv) Sei $1 \in \mathrm{End}(V), x \to x$. Sei außerdem $f \in \mathrm{End}(V)$, und $x \in V$ beliebig. Es gilt

$$f \circ 1 = 1 \circ f = f,$$

also End(V) ist ein Ring mit 1.

(b) V ist eine abelsche Gruppe (das haben wir vorausgesetzt). Wir müssen nur die andere Axiome betrachten. In folgendes Sei $\lambda, \mu \in K$ beliebiger Elemente von der Körper und $v, w \in V$. Weil K ein Körper ist, enthält K 1.

(i) $(\lambda \oplus \mu) \cdot v = \lambda \cdot v + \mu \cdot v$ folgt per Definition von $\oplus$.

(ii) $\lambda \cdot (v + w) = \lambda \cdot v + \lambda \cdot w$ gilt, weil λ ein Homomorphismus ist.

(iii)

$$\begin{aligned}(\lambda \circ \mu) \cdot v =& \lambda(\mu(v)) \\ =& \lambda \cdot (\mu \cdot v)\end{aligned}$$

(iv) Es gilt $1 \cdot v = 1(v) = v$ per Definition von 1. $\square$