

Lineare Algebra 1 Hausaufgabenblatt Nr. 4

Jun Wei Tan*

Julius-Maximilians-Universität Würzburg

(Dated: November 16, 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

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

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) Zeigen 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 eine Zahl k'_0 geben, mit $\deg(r_{k'_0}) = -\infty$.

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

$\deg(r_{k_0}) = -\infty$ 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 $\{0, 1, \dots, k'_0\}$ endlich ist, gibt es ein minimales Zahl k_0 mit der gewünschten Eigenschaft.

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

(b)

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

Sonst wäre es ein Widerspruch, weil k_0 nicht die kleinste Zahl mit dieser Eigenschaft wäre. Falls $r_{k_0} = 0$, wäre $k_0 - 1$ eine kleine Zahl mit der gewünschten 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 gemeinsame Teiler von a und b auch gemeinsame Teiler von a und b sind.

Jetzt nehmen wir an, dass es für eine beliebige $\mathbb{N} \ni k < k_0$ gilt, dass alle gemeinsame Teiler von r_k und r_{k-1} auch gemeinsame 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 gemeinsame Teiler p von r_{k_0} und r_{k_0-1} auch gemeinsame 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 $k \in \{0, 1, \dots, k_0\}$.

(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)

□

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 $K[t] \rightarrow \text{Abb}(K, K), f \rightarrow (x \rightarrow f(x))$ 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 $\deg(g) = 2$, 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

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

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

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

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)

□

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 $\mathbb{Z}/2\mathbb{Z} \rightarrow \mathbb{Z} : \bar{0} \cdot z = 0, \bar{1} \cdot z = z$ 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

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

- (c) Wahr. Ähnlich zu (a) folgt dies aus

□